Oikeustapauskokoelma

UNIONIN TUOMIOISTUIMEN TUOMIO (toinen jaosto)

19 päivänä lokakuuta 2016*

Ennakkoratkaisupyyntö — Henkilötietojen käsittely — Direktiivi 95/46/EY — 2 artiklan a alakohta — 7 artiklan f alakohta — Henkilötietojen käsite — Internetprotokollaosoitteet — Tallentaminen verkkomediapalvelujen tarjoajan toimesta — Kansallinen säännöstö, jonka mukaan rekisterinpitäjän oikeutettua intressiä ei voida ottaa huomioon

Asiassa C-582/14,

jossa on kyse SEUT 267 artiklaan perustuvasta ennakkoratkaisupyynnöstä, jonka Bundesgerichtshof (liittovaltion ylin tuomioistuin, Saksa) on esittänyt 28.10.2014 tekemällään päätöksellä, joka on saapunut unionin tuomioistuimeen 17.12.2014, saadakseen ennakkoratkaisun asiassa

**Patrick Breyer**

vastaan

**Saksan liittotasavalta,**

UNIONIN TUOMIOISTUIN (toinen jaosto),

toimien kokoonpanossa: jaoston puheenjohtaja M. Ilešič sekä tuomarit A. Prechal, A. Rosas (esittelevä tuomari), C. Toader, ja E. Jarašiūnas,

julkisasiamies: M. Campos Sánchez-Bordona,

kirjaaja: hallintovirkamies V. Giacobbo-Peyronnel,

ottaen huomioon kirjallisessa käsittelyssä ja 25.2.2016 pidetyssä istunnossa esitetyn,

ottaen huomioon huomautukset, jotka sille ovat esittäneet

— Patrick Breyer, edustajanaan M. Starostik, Rechtsanwalt,

— Saksan hallitus, asiamiehinään A. Lippstreu ja T. Henze,

— Itävallan hallitus, asiamiehenään G. Eberhard,

— Portugalin hallitus, asiamiehinään L. Inez Fernandes ja C. Vieira Guerra,

— Euroopan komissio, asiamiehinään P. J. O. Van Nuffel, H. Krämer, P. Costa de Oliveira ja J. Vondung,

* Oikeudenkäyntikieli: saksa.

kuultuaan julkisasiamiehen 12.5.2016 pidetyssä istunnossa esittämän ratkaisuehdotuksen,

on antanut seuraavan

**tuomion**

1 Ennakkoratkaisupyyntö koskee yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 24.10.1995 annetun Euroopan parlamentin ja neuvoston direktiivin 95/46/EY (EYVL 1995, L 281, s. 31) 2 artiklan a alakohdan ja 7 artiklan f alakohdan tulkintaa.

2 Tämä pyyntö on esitetty asiassa, jossa asianosaisina ovat Patrick Breyer ja Saksan liittotasavalta ja jossa on kyse siitä, että viimeksi mainittu on tallentanut ja säilyttänyt Breyerin internetprotokollaosoitteen (jäljempänä IP-osoite), kun tämä on käynyt useilla Saksan liittovaltion laitosten internetsivustoilla.

## Asiaa koskevat oikeussäännöt

### *Unionin oikeus*

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

”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.”

4 Mainitun direktiivin 1 artiklassa säädetään seuraavaa:

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

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

5 Kyseisen direktiivin 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 toimielintä, 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,

– –”

6 Direktiivin 95/46 3 artiklassa, jonka otsikko on ”Soveltamisala”, 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,

– –”

7 Mainitun direktiivin 5 artiklassa säädetään seuraavaa:

”Jäsenvaltioiden on määriteltävä henkilötietojen käsittelyn laillisuuden edellytykset tämän luvun säännösten rajoissa.”

8 Saman direktiivin 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 täytäntöön panemiseksi, 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.”

9 Direktiivin 95/46 13 artiklan 1 kohdassa säädetään seuraavaa:

”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

– –

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

– –”

*Saksan oikeus*

10 Sähköisistä tieto- ja viestintäpalveluista 26.2.2007 annetun lain (verkkomedialaki) (Telemediengesetz) (BGBl. 2007 I, s. 179; jäljempänä TMG) 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.”

11 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

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. – –”

12 Lisäksi 20.12.1990 annetun liittovaltion tietosuojalain (Bundesdatenschutzgesetz) (BGBl. 1990 I, s. 2954) 3 §:n 1 momentissa säädetään, että ”henkilötiedot ovat tunnistettua tai tunnistettavissa olevaa luonnollista henkilöä (rekisteröity) koskevia henkilökohtaisia tai asiallisia olosuhteita koskevia yksittäisiä tietoja – –”.

**Pääasia ja ennakkoratkaisukysymykset**

13 Breyer kävi useilla Saksan liittovaltion laitosten palvelusivustoilla. Kyseiset laitokset tarjoavat ajankohtaisia tietoja näillä yleisön saatavilla olevilla sivustoilla.

14 Verkkohyökkäyksiltä suojautumista ja hyökkääjien rikosoikeudelliseen vastuuseen saattamista varten useimmat näistä sivustoista tallentavat kaikki käynnit protokollatietoihin. Tietoihin tallennetaan myös käynnin päätyttyä haetun sivuston tai tiedoston nimi, hakukentissä käytetyt hakusanat, käynnin päivämäärä ja kellonaika, siirrettyjen tietojen määrä, ilmoitus sivustolle pääsyn onnistumisesta ja sen tietokoneen IP-osoite, jolta sivustolle on pyritty.

15 IP-osoitteet ovat verkossa oleville tietokoneille niiden internetin kautta tapahtuvan viestinnän helpottamiseksi annettuja numerosarjoja. Verkkosivulle pääsyä yritettäessä pääsyä yrittävän tietokoneen IP-osoite välittyy serverille, jolle tavoiteltu verkkosivu on tallennettu. Tämä on välttämätöntä, jotta pyydetyt tiedot välittyvät oikealle vastaanottajalle.

16 Ennakkoratkaisupyynnöstä ja unionin tuomioistuimen käytettävissä olevasta asiakirja-aineistosta käy lisäksi ilmi, että internetyhteyden tarjoajat antavat internetin käyttäjille joko staattisen IP-osoitteen tai dynaamisen IP-osoitteen eli IP-osoitteen, joka vaihtuu jokaisen uuden internetyhteyden ottamisen myötä. Toisin kuin staattiset IP-osoitteet, dynaamiset IP-osoitteet eivät mahdollista yleisesti saatavilla olevien tiedostojen avulla yhteyden toteamista tietyn tietokoneen ja internetpalvelun tarjoajan käyttämän fyysisen verkkoliittymän välillä.

17 Breyer nosti saksalaisessa hallintotuomioistuimessa kanteen, jossa hän vaati, että Saksan liittotasavaltaa kielletään tallentamasta tai antamasta sivullisen tallennettavaksi Saksan liittovaltion laitosten verkkomediapalveluiden yleisön saatavilla olevilla sivustoilla käynnin päätyttyä Breyerin isäntäjärjestelmän IP-osoitetta, jollei tallentaminen ole tarpeen verkkomediapalvelun käytettävyyden palauttamiseksi häiriön ilmetessä.

18 Koska Breyerin kanne hylättiin ensimmäisessä oikeusasteessa, hän haki muutosta hylkäävään päätökseen.

19 Toisen oikeusasteen tuomioistuin muutti kyseistä päätöstä osittain. Se määräsi Saksan liittotasavallan olemaan yksittäisen käytön päättymisen jälkeisen ajan osalta tallentamatta tai antamatta sivullisen tallennettavaksi Breyerin isäntäjärjestelmän IP-osoitetta, joka välittyy yleisön saatavilla internetissä olevien Saksan liittovaltion laitosten verkkomediapalvelujen käytön yhteydessä, jos osoite tallennetaan yhdessä sivustolla käynnin ajankohdan kanssa ja jos Breyer käytön yhteydessä antaa sellaisia tietoja, myös sähköpostiosoitteen muodossa, joiden avulla hänet voidaan tunnistaa, ja siltä osin kuin tallennus ei ole tarpeen verkkomediapalvelun käytettävyyden palauttamiseksi häiriön ilmetessä.

20 Toisen oikeusasteen tuomioistuimen mukaan dynaaminen IP-osoite yhdessä sivulla käynnin ajankohdan kanssa on silloin, kun asianomaisen internetsivuston käyttäjä on ilmaissut henkilöllisyytensä käynnin yhteydessä, henkilötieto, koska sivuston ylläpitäjä voi tunnistaa tämän käyttäjän yhdistämällä hänen nimensä hänen tietokoneensa IP-osoitteeseen.

21 Toisen oikeusasteen tuomioistuin katsoi, ettei Breyerin kannetta ollut syytä hyväksyä muiden tilanteiden osalta. Jos Breyer ei ilmaise henkilöllisyyttään sivustolla käynnin yhteydessä, vain internetyhteyden tarjoaja voi yhdistää IP-osoitteen tiettyyn liittymän haltijaan. Sen sijaan Saksan liittotasavallalle verkkomediapalvelujen tarjoajana IP-osoite ei ole henkilötieto edes yhdessä asianomaisen käyntikerran ajankohdan kanssa, koska tämä jäsenvaltio ei voi tunnistaa kyseisten internetsivustojen käyttäjää.

22 Sekä Breyer että Saksan liittotasavalta tekivät toisen oikeusasteen tuomioistuimen ratkaisusta Revision-valituksen Bundesgerichtshofiin (liittovaltion ylin tuomioistuin, Saksa). Breyer vaatii, että hänen kieltomääräystä koskeva vaatimuksensa hyväksytään kokonaisuudessaan. Saksan liittotasavalta vaatii tämän vaatimuksen hylkäämistä.

23 Ennakkoratkaisua pyytänyt tuomioistuin täsmentää, että Breyerin tietokoneen dynaamiset IP-osoitteet, jotka Saksan liittotasavalta tallentaa verkkomediapalvelujen tarjoajana, ovat ainakin muiden protokollatietoihin tallennettujen tietojen kontekstissa Breyerin asiallisia olosuhteita koskevia yksittäisiä tietoja, koska ne tarjoavat tietoja Breyerin käynneistä tietyillä internetsivustoilla tai -tiedostoissa tiettyinä ajankohtina.

24 Breyerin henkilöllisyyttä ei voida kuitenkaan tunnistaa suoraan näin tallennettujen tietojen perusteella. Pääasiassa kyseessä olevien internetsivustojen ylläpitäjät voivat tunnistaa Breyerin vain, jos tämän internetyhteyden tarjoaja välittää niille tämän käyttäjän henkilöllisyyttä koskevia tietoja. Näiden tietojen luokitteleminen henkilötiedoiksi riippuu näin ollen siitä, oliko Breyer tunnistettavissa.

25 Bundesgerichtshof tuo esiin oikeuskirjallisuudessa esiintyvät vastakkaiset näkemykset siitä, onko sen määrittämiseksi, onko henkilö tunnistettavissa, nojauduttava ”objektiiviseen” vai ”suhteelliseen” perusteeseen. Objektiivisen perusteen soveltamisesta seuraa, että pääasiassa kyseessä olevan IP-osoitteen kaltaisten tietojen voitaisiin internetsivustoilla käyntikerran päätyttyä katsoa olevan henkilötietoja siitä huolimatta, että ainoastaan sivullinen kykenee määrittämään rekisteröidyn henkilöllisyyden; tämä sivullinen on tässä tapauksessa Breyerin internetyhteyden tarjoaja, joka on tallentanut lisätietoja, jotka mahdollistavat hänen tunnistamisensa mainittujen IP-osoitteiden avulla. Suhteellisen perusteen mukaan näitä tietoja voidaan pitää henkilötietoina Breyerin internetyhteyden tarjoajan kaltaiseen elimeen nähden, koska niiden avulla käyttäjä on mahdollista tunnistaa täsmällisesti (ks. tältä osin tuomio 24.11.2011, Scarlet Extended, C-70/10, EU:C:201:771, 51 kohta), mutta niitä ei voida pitää tällaisina niiden internetsivustojen ylläpitäjän, joilla Breyer on käynyt, kaltaiseen toiseen elimeen nähden, koska tällä ylläpitäjällä ei ole silloin, kun Breyer ei ole ilmaissut henkilöllisyyttään sivustoilla käyntien yhteydessä, ilman suhteetonta vaivaa käytettävissään hänen tunnistamisekseen tarvittavia tietoja.

26 Siinä tapauksessa, että Breyerin tietokoneen dynaamisia IP-osoitteita olisi yhdessä asianomaisen käyntikerran ajankohdan kanssa pidettävä henkilötietoina, ennakkoratkaisua pyytänyt tuomioistuin pyrkii selvittämään, onko näiden IP-osoitteiden säilyttäminen sivustoilla käynnin päätyttyä sallittua direktiivin 7 artiklan f alakohdan nojalla.

27 Bundesgerichtshof täsmentää tältä osin, että yhtäältä verkkomediapalvelujen tarjoaja saa TMG:n 15 §:n 1 momentin mukaan kerätä ja hyödyntää käyttäjän henkilötietoja vain, kun se on tarpeen verkkomediapalvelujen käyttämisen mahdollistamiseksi ja niiden käytöstä laskuttamiseksi. Sama tuomioistuin toteaa toisaalta, että Saksan liittotasavallan mukaan näiden tietojen tallentaminen ja säilyttäminen ovat tarpeen sen yleisön saataville asettamien verkkomediapalvelujen sivustojen turvallisuuden ja toimivuuden takaamiseksi ja ylläpitämiseksi, kun sillä mahdollistetaan erityisesti se,

että tunnistetaan ja torjutaan niin sanotut palvelunestohyökkäykset, joilla sivustot lamautetaan siten, että tukitaan yksittäiset verkkoserverit käyttämällä kohdennetusti ja koordinoidusti suurta määrää tiedusteluja.

28 Ennakkoratkaisupyynnön esittänyt tuomioistuin toteaa, että jos ja siltä osin kuin edellytetään verkkomediapalvelujen tarjoajan toimenpiteitä tällaisilta hyökkäyksiltä suojautumiseksi, näitä toimenpiteitä voidaan tämän vuoksi pitää välttämättöminä ”sähköisten tieto- ja viestintäpalvelujen käyttämiseksi” TMG:n 15 §:ssä tarkoitetuin tavoin. Kirjallisuudessa vallitsevan näkemyksen mukaan on kuitenkin niin, että internetsivuston käyttäjän henkilötietojen kerääminen ja käyttö on sallittua vain tämän sivuston konkreettisen käytön mahdollistamiseksi ja että tiedot on kulloisenkin yksittäisen käytön päätyttyä poistettava, jolleivät ne ole tarpeen laskutusta varten. TMG:n 15 §:n 1 momentin tällä tavoin suppeasti tulkitseminen on kuitenkin esteenä sille, että IP-osoitteiden tallentaminen olisi sallittua tieto- ja viestintäpalvelujen turvallisuuden ja toimivuuden takaamiseksi yleisesti.

29 Ennakkoratkaisua pyytänyt tuomioistuin pohtii, onko tämä viimeksi mainittu tulkinta, jota toisen oikeusasteen tuomioistuin suosittelee, direktiivin 95/46 7 artiklan f alakohdan mukainen erityisesti niiden perusteiden valossa, jotka unionin tuomioistuin esitti 24.11.2011 antamansa tuomion ASNEF ja FECEMD (C-468/10 ja C-469/10, EU:C:2011:777) 29 kohdassa ja sitä seuraavissa kohdissa.

30 Näissä olosuhteissa Bundesgerichtshof on päättänyt lykätä asian käsittelyä ja esittää unionin tuomioistuimelle seuraavat ennakkoratkaisukysymykset:

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

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

## Ennakkoratkaisukysymysten tarkastelu

### *Ensimmäinen kysymys*

31 Ennakkoratkaisua pyytänyt tuomioistuin tiedustelee ensimmäisellä kysymyksellään, onko direktiivin 95/46 2 artiklan a alakohtaa tulkittava siten, että dynaaminen IP-osoite, jonka verkkomediapalvelun tarjoaja tallentaa henkilön käydessä tämän palveluntarjoajan yleisön saataville asettamalla internetsivustolla, on tähän palveluntarjoajaan nähden kyseisessä säännöksessä tarkoitettu henkilötieto, jos vain sivullisella, tässä tapauksessa tämän henkilön internetyhteyden tarjoajalla, on käytettävissään hänen tunnistamisekseen tarvittavia lisätietoja.

32 Kyseisen säännöksen mukaan henkilötiedoilla tarkoitetaan ”kaikenlaisia tunnistettua tai tunnistettavissa olevaa luonnollista henkilöä (’rekisteröity’) koskevia tietoja”. Säännöksen mukaan 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.

33 On aluksi todettava, että 24.11.2011 annetun tuomion Scarlet Extended (C-70/10, EU:C:2011:771), joka koski muun muassa direktiivin 95/46 tulkintaa, 51 kohdassa unionin tuomioistuin katsoi, että internetin käyttäjien IP-osoitteet ovat suojattuja henkilötietoja, koska niiden avulla mainitut käyttäjät on mahdollista tunnistaa täsmällisesti.

34 Tämä unionin tuomioistuimen toteamus koski kuitenkin tilannetta, jossa internetin käyttäjien IP-osoitteiden keräämisen ja tunnistamisen suorittivat internetyhteyden tarjoajat.

35 Käsiteltävässä asiassa ensimmäinen kysymys koskee tilannetta, jossa verkkomediapalvelujen tarjoaja eli Saksan liittotasavalta on se, joka tallentaa tämän palvelujentarjoajan yleisön saataville asettaman internetsivuston käyttäjien IP-osoitteet, eikä sillä ole käytettävissään näiden käyttäjien tunnistamiseksi tarvittavia lisätietoja.

36 On lisäksi riidatonta, että IP-osoitteet, joihin ennakkoratkaisua pyytänyt tuomioistuin viittaa, ovat dynaamisia IP-osoitteita eli toisin sanoen tilapäisiä osoitteita, jotka annetaan kunkin internetyhteyden yhteydessä ja jotka vaihtuvat myöhempien internetyhteyksien yhteydessä, eivätkä staattisia IP-osoitteita, jotka ovat muuttumattomia ja joiden perusteella verkkoyhteydessä oleva laite voidaan tunnistaa pysyvästi.

37 Ennakkoratkaisua pyytäneen tuomioistuimen ensimmäinen kysymys perustuu siis siihen lähtökohtaan, jonka mukaan yhtäältä tiedot, jotka koostuvat dynaamisesta IP-osoitteesta ja tästä IP-osoitteesta tapahtuneen internetsivustolla käynnin päivämäärästä ja kellonajasta ja jotka verkkomediapalvelujen tarjoaja tallentaa, eivät yksinään anna tälle palveluntarjoajalle mahdollisuutta tunnistaa kyseistä tällä internetsivustolla käynyttä käyttäjää, ja toisaalta internetyhteyden tarjoajalla puolestaan on käytettävissä lisätietoja, joiden perusteella on mahdollista tunnistaa tämä käyttäjä, kun niihin yhdistetään kyseinen IP-osoite.

38 Tältä osin on ensin todettava, että on kiistatonta, että dynaaminen IP-osoite ei ole ”tunnistettua luonnollista henkilöä” koskeva tieto, koska tällaisesta osoitteesta ei käy suoraan ilmi, kenelle luonnolliselle henkilölle tietokone, jolta internetsivustolla on käyty, kuuluu, eikä tällainen osoite paljasta suoraan muun mahdollisesti tätä tietokonetta käyttävän henkilön henkilöllisyyttä.

39 Sen ratkaisemiseksi, onko dynaaminen IP-osoite edellä 37 kohdassa tarkoitetussa tilanteessa direktiivin 96/45 2 artiklan a alakohdassa tarkoitettu henkilötieto verkkomediapalvelujen tarjoajiin nähden, on tutkittava, voidaanko tällaisen palveluntarjoajan tallentamaa dynaamista IP-osoitetta pitää ”tunnistettavissa olevaa luonnollista henkilöä” koskevana tietona, kun tämän palveluntarjoajan yleisön saataville asettaman internetsivuston käyttäjän tunnistamiseksi tarvittavat lisätiedot ovat kyseisen käyttäjän internetyhteyden tarjoajan hallussa.

40 Tältä osin direktiivin 95/46 2 artiklan a alakohdassa säädetään, että tunnistettavissa olevana pidetään henkilöä, joka voidaan tunnistaa paitsi suoraan myös epäsuorasti.

41 Se, että unionin lainsäätäjä käyttää sanaa ”epäsuorasti”, kertoo, että tiedon luokitteleminen henkilötiedoksi ei edellytä, että tämä tieto yksin mahdollistaa rekisteröidyn tunnistamisen.

42 Lisäksi direktiivin 95/46 johdanto-osan 26 perustelukappaleessa todetaan, että sen määrittämiseksi, onko henkilö tunnistettavissa, olisi otettava huomioon kaikki kohtuullisesti toteutettavissa olevat keinot, joita joko rekisterinpitäjä tai joku muu voi kyseisen henkilön tunnistamiseksi käyttää.

43 Siltä osin kuin tässä perustelukappaleessa viitataan kohtuullisesti toteuttavissa oleviin keinoihin, joita joko rekisterinpitäjä tai joku muu käyttää, sen sanamuoto viittaa siihen, että jotta tietoa voitaisiin pitää kyseisen direktiivin 2 artiklan a alakohdassa tarkoitettuna henkilötietona, ei edellytetä, että kaikki tiedot, joiden perusteella rekisteröity voidaan tunnistaa, ovat yhden ainoan tahon hallussa.

44 Se, että internetsivuston käyttäjän tunnistamiseksi tarvittavat lisätiedot eivät ole verkkomediapalvelujen tarjoajan vaan kyseisen käyttäjän internetyhteyden tarjoajan hallussa, ei siis näytä sulkevan pois sitä, että verkkomediapalvelujen tarjoajan tallentamat dynaamiset IP-osoitteet ovat sen kannalta direktiivin 95/46 2 artiklan a alakohdassa tarkoitettuja henkilötietoja.

45 On kuitenkin selvitettävä, onko mahdollisuus yhdistää dynaaminen IP-osoite mainittuihin internetyhteyden tarjoajan hallussa oleviin lisätietoihin edellä mainittu rekisteröidyn tunnistamiseksi kohtuullisesti toteutettavissa oleva keino.

46 Kuten julkisasiamies on todennut ratkaisuehdotuksensa 68 kohdassa, näin ei ole silloin, kun rekisteröidyn tunnistaminen on kielletty laissa tai kun se ei ole käytännössä toteutettavissa esimerkiksi siitä syystä, että se veisi suhteettomasti aikaa ja aiheuttaisi suhteettomasti kustannuksia ja työtä, minkä seurauksena tunnistamisen riski näyttäytyy käytännössä merkityksettömänä.

47 Vaikka ennakkoratkaisua pyytänyt tuomioistuin täsmentää ennakkoratkaisupyynnössään, että Saksan lainsäädännön mukaan internetyhteyden tarjoaja ei saa siirtää suoraan verkkomediapalvelujen tarjoajalle rekisteröidyn tunnistamisen kannalta tarpeellisia lisätietoja, vaikuttaa kuitenkin siltä – jollei kyseisen tuomioistuimen tältä osin suoritettavista tarkastuksista muuta johdu –, että olemassa on laillisia keinoja, joiden avulla verkkomediapalvelujen tarjoaja voi kääntyä erityisesti kyberhyökkäystilanteessa toimivaltaisen viranomaisen puoleen, jotta tämä ryhtyy tarvittaviin toimiin näiden tietojen hankkimiseksi internetyhteyden tarjoajalta ja käynnistää rikosoikeudellisen menettelyn.

48 Näin ollen vaikuttaa siltä, että verkkomediapalvelujen tarjoajalla on käytettävissään kohtuullisesti toteutettavissa olevat keinot rekisteröidyn tunnistamiseksi tallennettujen IP-osoitteiden perusteella muiden tahojen eli toimivaltaisen viranomaisen ja internetyhteyden tarjoajan avulla.

49 Kaiken edellä esitetyn perusteella ensimmäiseen kysymykseen on vastattava, että direktiivin 95/46 2 artiklan a alakohtaa on tulkittava siten, että dynaaminen IP-osoite, jonka verkkomediapalvelujen tarjoaja tallentaa henkilön käydessä tämän palveluntarjoajan yleisön saataville asettamalla internetsivustolla, on tähän palveluntarjoajaan nähden kyseisessä säännöksessä tarkoitettu henkilötieto, jos palveluntarjoajalla on käytettävissään oikeudelliset keinot, joiden perusteella se voi tunnistaa kyseisen henkilön sellaisten lisätietojen avulla, jotka ovat tämän henkilön internetyhteyden tarjoajan käytettävissä.

*Toinen kysymys*

50 Ennakkoratkaisua pyytänyt tuomioistuin kysyy toisella kysymyksellään, onko direktiivin 95/46 7 artiklan f alakohtaa tulkittava siten, että se on esteenä sellaiselle jäsenvaltion säännöstölle, jonka nojalla verkkomediapalvelujen tarjoaja saa kerätä ja hyödyntää näiden palvelujen käyttäjän henkilötietoja ilman tämän suostumusta vain silloin, kun kerääminen ja hyödyntäminen ovat tarpeen, jotta mahdollistetaan kyseisen käyttäjän kyseisten palvelujen tosiasiallinen käyttö ja tämän käytön laskutus, ja jonka mukaan palvelujen yleisen toiminnan takaamisen tavoitteella ei voida oikeuttaa kulloisenkin yksittäisen käytön päättymisen jälkeistä näiden tietojen hyödyntämistä.

51 Ennen tähän kysymykseen vastaamista on ratkaistava, onko pääasiassa kyseessä oleva henkilötietojen eli eräiden Saksan liittovaltion laitosten internetsivustojen käyttäjien dynaamisten IP-osoitteiden käsittely suljettu direktiivin 95/46 soveltamisalan ulkopuolelle direktiivin 3 artiklan 2 kohdan ensimmäisen luetelmakohdan nojalla; sen mukaan direktiiviä ei sovelleta henkilötietojen käsittelyyn, joka koskee muun muassa rikosoikeuden alalla tapahtuvaa valtion toimintaa.

52 Tältä osin on palautettava mieleen, että kyseisessä säännöksessä esimerkkeinä mainitut toiminnat ovat kaikki valtiolle tai valtion viranomaisille tyypillisiä toimintoja, jotka eivät liity yksityisten henkilöiden toiminta-aloihin (ks. tuomio 6.11.2003, Lindqvist, C-101/01, EU:C:2003:596, 43 kohta ja tuomio 16.12.2008, Satakunnan Markkinapörssi ja Satamedia, C-73/07, EU:C:2008:727, 41 kohta).

53 Jollei ennakkoratkaisua pyytäneen tuomioistuimen suoritettavista tarkistuksista muuta johdu, pääasiassa tilanne vaikuttaa siltä, että Saksan liittovaltion laitokset, jotka tarjoavat verkkomediapalveluja ja jotka ovat vastuussa dynaamisten IP-osoitteiden käsittelystä, toimivat julkisen viranomaisen asemastaan huolimatta yksityisessä ominaisuudessa ja rikosoikeuden alalla tapahtuvan jäsenvaltioiden toiminnan ulkopuolella.

54 On siis tutkittava, onko pääasiassa kyseessä olevan kaltainen jäsenvaltion säännöstö yhteensopiva direktiivin 95/46 7 artiklan f alakohdan kanssa.

55 Tätä varten on palautettava mieleen, että pääasiassa kyseessä olevassa kansallisessa säännöstössä, kun sitä tulkitaan ennakkoratkaisua pyytäneen tuomioistuimen esittämin tavoin suppeasti, sallitaan mainittujen palvelujen käyttäjän henkilötietojen kerääminen ja hyödyntäminen ilman tämän suostumusta vain silloin, kun tämä on tarpeen, jotta mahdollistetaan kyseisen käyttäjän kyseisen palvelun tosiasiallinen käyttö ja tämän käytön laskutus, eikä verkkomediapalvelun yleisen toiminnan takaamisen tavoitteella voida oikeuttaa kulloisenkin yksittäisen käytön päättymisen jälkeistä näiden tietojen hyödyntämistä.

56 Direktiivin 95/46 7 artiklan f alakohdan mukaan henkilötietojen käsittely on laillista, jos käsittely on tarpeen rekisterinpitäjän tai tiedot saavan sivullisen oikeutetun intressin toteuttamiseksi, paitsi milloin tämän intressin syrjäyttävät rekisteröidyn kyseisen direktiivin 1 artiklan 1 kohdan perusteella suojaa tarvitsevat intressit ja perusoikeudet ja -vapaudet.

57 Unionin tuomioistuin on jo todennut, että kyseisen direktiivin 7 artiklaan on otettu tyhjentävä luettelo, johon on rajattu tilanteet, joissa henkilötietojen käsittelyn voidaan katsoa olevan laillista, ja että jäsenvaltiot eivät voi lisätä direktiivin kyseiseen artiklaan uusia henkilötietojen käsittelyn laillistamista koskevia periaatteita eivätkä säätää lisävaatimuksista, joilla muutettaisiin jonkin niiden kuuden periaatteen ulottuvuutta, joista tässä artiklassa on säädetty (ks. vastaavasti tuomio 24.11.2011, ASNEF ja FECEMD, C-468/10 ja C-469/10, EU:C:2011:777, 30 ja 32 kohta).

58 Vaikka direktiivin 95/46 5 artiklassa annetaan jäsenvaltioille lupa määritellä henkilötietojen käsittelyn laillisuuden edellytykset ainoastaan direktiivin II luvussa eli näin siis sen 7 artiklassa säädetyissä rajoissa, harkintavaltaa, joka jäsenvaltioilla on direktiivin 5 artiklan nojalla, voidaan käyttää ainoastaan kyseisen direktiivin sen tavoitteen mukaisesti, joka koskee henkilötietojen vapaan liikkuvuuden ja yksityiselämän suojan välisen tasapainon säilyttämistä. Jäsenvaltiot eivät voi myöskään kyseisen direktiivin 5 artiklan 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 (ks. vastaavasti tuomio 24.11.2011, ASNEF ja FECEMD, C-468/10 ja C-469/10, EU:C:2011:777, 33, 34 ja 36 kohta).

59 Käsiteltävässä asiassa on ilmeistä, että TMG:n 15 §:llä – jos sitä tulkitaan edellä 55 kohdassa mainituin tavoin suppeasti – on suppeampi ulottuvuus kuin direktiivin 95/46 7 artiklan f alakohdassa säädetyllä periaatteella.

60 Kun kyseisen direktiivin 7 artiklan f alakohdassa viitataan yleisesti rekisterinpitäjän tai tiedot saavan sivullisen oikeutetun intressin toteuttamiseen, TMG:n 15 §:ssä annetaan palveluntarjoajalle lupa kerätä ja hyödyntää käyttäjän henkilötietoja vain silloin, kun tämä on tarpeen, jotta mahdollistetaan kyseisen käyttäjän verkkomediapalvelujen tosiasiallinen käyttö ja tämän käytön laskutus. TMG:n 15 § on siis yleisesti esteenä sille, että verkkomediapalvelujen yksittäisen käytön päättymisen jälkeen säilytetään henkilötietoja näiden palvelujen käyttämisen takaamiseksi. Saksan liittovaltion laitoksilla, jotka tarjoavat

verkkomediapalveluja, voi kuitenkin myös olla oikeutettu intressi mainittujen sivustojen toiminnan jatkuvuuden takaamiseen niiden yleisön saatavilla olevien internetsivustojen kunkin konkreettisen yksittäisen käytön lisäksi.

61 Kuten julkisasiamies on todennut ratkaisuehdotuksensa 100 ja 101 kohdassa, tässä kansallisessa säännöstössä ei ole pelkästään täsmennetty direktiivin 95/46 5 artiklan mukaisesti direktiivin 7 artiklan f alakohtaan sisältyvää oikeutetun intressin käsitettä.

62 Tältä osin on muistettava myös, että direktiivin 7 artiklan f alakohta on esteenä sille, että jäsenvaltio sulkee ehdottomasti ja yleisesti pois mahdollisuuden käsitellä tiettyihin tietoryhmiin kuuluvia henkilötietoja sallimatta niiden oikeuksien ja intressien punnitsemista, joista on kyse tietyssä yksittäisessä tapauksessa. Jäsenvaltio ei voi siis näiden ryhmien osalta vahvistaa lopullisesti, mikä vastakkaisten oikeuksien ja intressien punnitsemisen tulos on, sallimatta muunlaista tulosta tiettyjen konkreettisessa tapauksessa vallitsevien erityisten olosuhteiden perusteella (ks. vastaavasti tuomio 24.11.2011, ASNEF ja FECEMD, C-468/10 ja C-469/10, EU:C:2011:777, 47 ja 48 kohta).

63 Pääasiassa kyseessä olevalla säännöstöllä rajoitetaan verkkomediapalvelujen sivustojen käyttäjien henkilötietojen käsittelyn osalta direktiivin 95/46 7 artiklan f alakohdassa vahvistetun periaatteen ulottuvuutta, kun siinä suljetaan pois se, että verkkomediapalvelun yleisen toiminnan takaamisen tavoitetta voitaisiin punnita suhteessa näiden käyttäjien intresseihin tai perusoikeuksiin ja -vapauksiin, jotka kyseisen direktiivin 1 artiklan 1 kohdan perusteella tarvitsevat suojaa.

64 Kaiken edellä esitetyn perusteella toiseen kysymykseen on vastattava, että direktiivin 95/46 7 artiklan f alakohtaa on tulkittava siten, että se on esteenä sellaiselle jäsenvaltion säännöstölle, jonka nojalla verkkomediapalvelujen tarjoaja saa kerätä ja hyödyntää näiden palvelujen käyttäjän henkilötietoja ilman tämän suostumusta vain silloin, kun kerääminen ja hyödyntäminen ovat tarpeen, jotta mahdollistetaan kyseisen käyttäjän kyseisten palvelujen tosiasiallinen käyttö ja tämän käytön laskutus, ja jonka mukaan palvelujen yleisen toiminnan takaamisen tavoitteella ei voida oikeuttaa kulloisenkin yksittäisen käytön päättymisen jälkeistä näiden tietojen hyödyntämistä.

## Oikeudenkäyntikulut

65 Pääasian asianosaisten osalta asian käsittely unionin tuomioistuimessa on välivaihe kansallisessa tuomioistuimessa vireillä olevan asian käsittelyssä, minkä vuoksi kansallisen tuomioistuimen asiana on päättää oikeudenkäyntikulujen korvaamisesta. Oikeudenkäyntikuluja, jotka ovat aiheutuneet muille kuin näille asianosaisille huomautusten esittämisestä unionin tuomioistuimelle, ei voida määrätä korvattaviksi.

Näillä perusteilla unionin tuomioistuin (toinen jaosto) on ratkaissut asian 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 alakohtaa on tulkittava siten, että dynaaminen internetprotokollaosoite, jonka verkkomediapalvelujen tarjoaja tallentaa henkilön käydessä tämän palveluntarjoajan yleisön saataville asettamalla internetsivustolla, on tähän palveluntarjoajaan nähden kyseisessä säännöksessä tarkoitettu henkilötieto, jos palveluntarjoajalla on käytettävissään oikeudelliset keinot, joiden perusteella se voi tunnistaa kyseisen henkilön sellaisten lisätietojen avulla, jotka ovat tämän henkilön internetyhteyden tarjoajan käytettävissä.**

2) **Direktiivin 95/46 7 artiklan f alakohtaa on tulkittava siten, että se on esteenä sellaiselle jäsenvaltion säännöstölle, jonka nojalla verkkomediapalvelujen tarjoaja saa kerätä ja hyödyntää näiden palvelujen käyttäjän henkilötietoja ilman tämän suostumusta vain silloin, kun kerääminen ja hyödyntäminen ovat tarpeen, jotta mahdollistetaan kyseisen käyttäjän**

**kyseisten palvelujen tosiasiallinen käyttö ja tämän käytön laskutus, ja jonka mukaan palvelujen yleisen toiminnan takaamisen tavoitteella ei voida oikeuttaa kulloisenkin yksittäisen käytön päättymisen jälkeistä näiden tietojen hyödyntämistä.**

Allekirjoitukset