Rättsfallssamlingen

DOMSTOLENS DOM (andra avdelningen)

den 19 oktober 2016*

”Begäran om förhandsavgörande — Behandling av personuppgifter — Direktiv 95/46/EG — Artikel 2 a — Artikel 7 f — Begreppet personuppgifter — IP-adresser — Lagring som görs av den som tillhandahåller elektroniska informations- eller kommunikationstjänster — Nationell lagstiftning enligt vilken det inte är möjligt att beakta den registeransvariges berättigade intresse”

I mål C-582/14,

angående en begäran om förhandsavgörande enligt artikel 267 FEUF, framställd av Bundesgerichtshof (Federala högsta domstolen, Tyskland) genom beslut av den 28 oktober 2014, som inkom till domstolen den 17 december 2014, i målet

Patrick Breyer

mot

Bundesrepublik Deutschland,

meddelar

DOMSTOLEN (andra avdelningen)

sammansatt av avdelningsordföranden M. Ilešič samt domarna A. Prechal, A. Rosas (referent), C. Toader och E. Jarašiūnas,

generaladvokat: M. Campos Sánchez-Bordona

justitiesekreterare: handläggaren V. Giacobbo-Peyronnel,

efter det skriftliga förfarandet och förhandlingen den 25 februari 2016,

med beaktande av de yttranden som avgetts av:

— Patrick Breyer, genom M. Starostik, Rechtsanwalt,

— Tysklands regering, genom A. Lippstreu och T. Henze, båda i egenskap av ombud,

— Österrikes regering, genom G. Eberhard, i egenskap av ombud,

— Portugals regering, genom L. Inez Fernandes och C. Vieira Guerra, båda i egenskap av ombud,

* Rättegångsspråk: tyska

— Europeiska kommissionen, genom P.J.O. Van Nuffel, H. Krämer, P. Costa de Oliveira och J. Vondung, samtliga i egenskap av ombud,

och efter att den 12 maj 2016 ha hört generaladvokatens förslag till avgörande,

följande

Dom

1 Begäran om förhandsavgörande avser tolkningen av artikel 2 a och artikel 7 f i Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (EGT L 281, 1995, s. 31).

2 Begäran har framställts i ett mål mellan Patrick Breyer och Bundesrepublik Deutschland (Förbundsrepubliken Tyskland) angående den registrering och lagring av Patrick Breyers IP-adress som den medlemsstaten genomförde i samband med att Patrick Breyer besökte ett flertal webbplatser som drivs av tyska federala myndigheter.

Tillämpliga bestämmelser

Unionsrätt

3 Skäl 26 i direktiv 95/46 har följande lydelse:

”Principerna för skyddet måste gälla all information som rör en identifierad eller identifierbar person. För att avgöra om en person är identifierbar skall härvid beaktas alla hjälpmedel som i syfte att identifiera vederbörande rimligen kan komma att användas antingen av den registeransvarige eller av någon annan person. Skyddsprinciperna gäller inte för uppgifter som gjorts anonyma på ett sådant sätt att den registrerade inte längre är identifierbar. En sådan uppförandekodex som avses i artikel 27 kan vara ett användbart redskap för att ge vägledning om hur uppgifter kan göras anonyma och behållas i en form som gör det omöjligt att identifiera den registrerade.”

4 I artikel 1 i direktivet föreskrivs följande:

”1. Medlemsstaterna skall i enlighet med detta direktiv skydda fysiska personers grundläggande fri- och rättigheter, särskilt rätten till privatliv, i samband med behandling av personuppgifter.

2. Medlemsstaterna får varken begränsa eller förbjuda det fria flödet av personuppgifter mellan medlemsstaterna av skäl som har samband med det under punkt 1 föreskrivna skyddet.”

5 Artikel 2 i samma direktiv har följande lydelse:

”I detta direktiv avses med

a) *personuppgifter*: varje upplysning som avser en identifierad eller identifierbar fysisk person (den registrerade). En identifierbar person är en person som kan identifieras, direkt eller indirekt, framför allt genom hänvisning till ett identifikationsnummer eller till en eller flera faktorer som är specifika för hans fysiska, fysiologiska, psykiska, ekonomiska, kulturella eller sociala identitet,

b) *behandling av personuppgifter (behandling)*: varje åtgärd eller serie av åtgärder som vidtas beträffande personuppgifter, vare sig det sker på automatisk väg eller inte, till exempel insamling, registrering, organisering, lagring, bearbetning eller ändring, återvinning, inhämtande, användning, utlämnande genom översändande, spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning, blockering, utplåning eller förstöring,

…

d) *registeransvarig*: den fysiska eller juridiska person, den myndighet, den institution eller det andra organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. När ändamålen och medlen för behandlingen bestäms av nationella lagar och andra författningar eller av gemenskapsrätten kan den registeransvarige eller de särskilda kriterierna för att utse honom anges i nationell rätt eller i gemenskapsrätten,

…

f) *tredje man*: [varje annan fysisk eller juridisk person, myndighet, institution eller annat organ] än den registrerade, den registeransvarige, registerföraren och de personer som under den registeransvariges eller registerförarens direkta ansvar har befogenhet att behandla uppgifterna,

…”

6 Artikel 3 i direktiv 95/46, med rubriken ”Tillämpningsområde”, har följande lydelse:

”1. Detta direktiv gäller för sådan behandling av personuppgifter som helt eller delvis företas på automatisk väg liksom för annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register.

2. Detta direktiv gäller inte för sådan behandling av personuppgifter

— som utgör ett led i en verksamhet som inte omfattas av gemenskapsrätten, exempelvis sådan verksamhet som avses i avdelningarna V och VI i Fördraget om Europeiska unionen, och inte under några omständigheter behandlingar som rör allmän säkerhet, försvar, statens säkerhet (inbegripet statens ekonomiska välstånd när behandlingen har samband med frågor om statens säkerhet) och statens verksamhet på straffrättens område,

…”

7 Artikel 5 i nämnda direktiv har följande lydelse:

”Medlemsstaterna skall inom de begränsningar som bestämmelserna i detta kapitel innebär, precisera på vilka villkor behandling av personuppgifter är tillåten.”

8 Artikel 7 i direktivet har följande lydelse:

”Medlemsstaterna skall föreskriva att personuppgifter får behandlas endast om

a) den registrerade otvetydigt har lämnat sitt samtycke, eller

b) behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås, eller

c) behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den registeransvarige, eller

d) behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade,

e) behandlingen är nödvändig för att utföra en arbetsuppgift av allmänt intresse eller som är ett led i myndighetsutövning som utförs av den registeransvarige eller tredje man till vilken uppgifterna har lämnats ut, eller

f) behandlingen är nödvändig för ändamål som rör berättigade intressen hos den registeransvarige eller hos den eller de tredje män till vilka uppgifterna har lämnats ut, utom när sådana intressen uppvägs av den registrerades intressen eller dennes grundläggande fri- och rättigheter som kräver skydd under artikel 1.1."

9 Artikel 13.1 i direktiv 95/46 har följande lydelse:

"Medlemsstaterna får genom lagstiftning vidta åtgärder för att begränsa omfattningen av de skyldigheter och rättigheter som anges i artiklarna 6.1, 10, 11.1, 12 och 21 i fall då en sådan begränsning är en nödvändig åtgärd med hänsyn till

…

d) förebyggande, undersökning, avslöjande av brott eller åtal för brott eller av överträdelser av etiska regler som gäller för lagreglerade yrken,

…"

Tysk rätt

10 I 12 § Telemediengesetz (lagen om elektroniska informations- och kommunikationstjänster) av den 26 februari 2007 (BGBl. 2007 I, s. 179) (nedan kallad TMG) föreskrivs följande:

"1) Tjänsteleverantören får samla in och behandla personuppgifter för att tillhandahålla elektroniska informations- eller kommunikationstjänster endast om detta är tillåtet enligt denna lag eller annan föreskrift som uttryckligen avser sådana tjänster, eller om användaren har gett sitt samtycke.

2) Tjänsteleverantören får använda personuppgifter som samlats in för att tillhandahålla elektroniska informations- eller kommunikationstjänster för andra syften endast om det är tillåtet enligt denna lag eller annan föreskrift som uttryckligen avser sådana tjänster, eller om användaren har gett sitt samtycke.

3) Om inte annat föreskrivs ska gällande bestämmelser om skydd för personuppgifter tillämpas även när uppgifterna inte behandlas genom automatisk databehandling."

11 I 15 § TMG föreskrivs följande:

"1) Tjänsteleverantören får samla in och använda en användares personuppgifter endast i den mån det krävs för att möjliggöra och fakturera användningen av de elektroniska informations- eller kommunikationstjänsterna (användningsdata). Med användningsdata avses särskilt

1. uppgifter som gör det möjligt att identifiera användaren,

2. uppgifter om när den aktuella användningen inleddes och avslutades, samt dess omfattning, och

3. uppgifter om de elektroniska informations- eller kommunikationstjänster som användaren använt.

2) Tjänsteleverantören får sammanföra en användares användningsdata avseende olika elektroniska informations- eller kommunikationstjänster i den mån det krävs för att fakturera användaren.

…

4) Tjänsteleverantören får använda användningsdata efter det att sessionen avslutats i den mån det krävs för att fakturera användaren för tjänsten (faktureringsdata). Tjänsteleverantören kan låsa dessa data för att iaktta de längsta lagringstider som följer av lagar, förordningar eller avtal. …”

12 I 3 § stycke 1 Bundesdatenschutzgesetz (federala dataskyddslagen) av den 20 december 1990 (BGBl. 1990 I, s. 2954) föreskrivs att ”[p]ersonuppgifter är uppgifter angående personliga eller faktiska omständigheter avseende en identifierad eller identifierbar fysisk person (den registrerade). …”

Målet vid den nationella domstolen och tolkningsfrågorna

13 Patrick Breyer besökte flera webbplatser som drivs av tyska federala myndigheter. På webbplatserna, som är tillgängliga för allmänheten, ges aktuell information.

14 I syfte att avvärja attacker och möjliggöra lagföring av hackare lagras för de flesta av dessa webbplatser alla besök i loggfiler. I loggfilerna lagras, efter sessionens slut, namnet på den besökta webbplatsen eller filen, de sökord som angetts i sökfält, datum och klockslag för besöket, överförd datamängd, uppgift om huruvida försöket till åtkomst lyckades, och IP-adressen för den dator från vilken åtkomst söktes.

15 IP-adresser är siffersträngar som tilldelas datorer som är uppkopplade till internet, för att de ska kunna kommunicera via internet. När någon besöker en webbplats överförs avsändardatorns IP-adress till den server på vilken den aktuella webbplatsen är lagrad. Detta är nödvändigt för att de eftersökta uppgifterna ska kunna överföras till rätt mottagare.

16 Det framgår vidare av beslutet om hänskjutande och av handlingarna i målet att internetleverantörerna tilldelar internetanvändarnas datorer antingen en ”statisk” eller en ”dynamisk” IP-adress. Den sistnämnda ändras vid varje ny uppkoppling till internet. Till skillnad från statiska IP-adresser är det inte möjligt att med en dynamisk IP-adress göra en koppling, med hjälp av allmänt tillgängliga filer, mellan en viss dator och den fysiska anslutning till nätverket som internetleverantören använder.

17 Patrick Breyer väckte talan vid tysk förvaltningsdomstol och yrkade att Förbundsrepubliken Tyskland skulle förbjudas att lagra eller uppdra åt tredje man att lagra IP-adressen till Patrick Breyers värdsystem, efter varje besök på tyska federala myndigheters allmänt tillgängliga webbplatser för elektroniska informations- eller kommunikationstjänster, i den mån lagringen inte är nödvändig för att i händelse av avbrott återställa tillgången till tjänsterna.

18 Patrick Breyer överklagade avgörandet i första instans varigenom hans talan ogillades.

19 Domstolen i andra instans ändrade det avgörandet i vissa delar. Sålunda förpliktades Förbundsrepubliken Tyskland att avhålla sig från att lagra eller uppdra åt tredje man att, efter varje besök, lagra IP-adressen till Patrick Breyers värdsystem, vilken överförts i samband med att han besökte tyska federala myndigheters allmänt tillgängliga webbplatser för elektroniska informations- eller kommunikationstjänster, för det fall adressen lagras tillsammans med uppgift om datum för den session för vilken IP-adressen användes och för det fall Patrick Breyer under sessionen har uppgett sin identitet, inbegripet i form av en elektronisk adress där hans identitet anges. Detta gällde i den mån lagringen inte är nödvändig för att i händelse av avbrott återställa tillgången till de elektroniska informations- eller kommunikationstjänsterna.

20 Enligt domstolen i andra instans utgör en dynamisk IP-adress tillsammans med uppgift om datum för den session för vilken IP-adressen använts, en personuppgift när den som har använt den aktuella webbplatsen har uppgett sin identitet under sessionen. Den som driver webbplatsen kan nämligen identifiera användaren genom att koppla samman användarens namn med IP-adressen till dennes dator.

21 Domstolen i andra instans ansåg emellertid inte att det fanns skäl att bifalla Patrick Breyers yrkande såvitt gäller andra situationer. I den situationen där han inte uppger sin identitet under ett besök på en webbplats är det nämligen endast internetleverantören som kan koppla samman IP-adressen med en bestämd innehavare av ett internetabonnemang. Om det är Förbundsrepubliken Tyskland, i dess egenskap av leverantör av elektroniska informations- eller kommunikationstjänster, som innehar uppgiften om IP-adressen skulle denna däremot inte utgöra en personuppgift, ens tillsammans med en uppgift om datum för den session för vilken IP-adressen använts, eftersom medlemsstaten inte skulle kunna identifiera användaren av de aktuella webbplatserna.

22 Patrick Breyer och Förbundsrepubliken Tyskland har båda överklagat detta avgörande till Bundesgerichtshof (Federala högsta domstolen, Tyskland). Patrick Breyer har yrkat att hans talan om förbudsföreläggande ska bifallas i sin helhet. Förbundsrepubliken Tyskland har yrkat att Patrick Breyers talan ska ogillas i sin helhet.

23 Den hänskjutande domstolen har angett att de dynamiska IP-adresserna till Patrick Breyers dator, vilka Förbundsrepubliken Tyskland har lagrat i sin egenskap av leverantör av elektroniska informations- eller kommunikationstjänster, utgör, åtminstone i förening med andra uppgifter som lagras i loggfiler, särskilda uppgifter om faktiska omständigheter rörande Patrick Breyer, eftersom uppgifterna ger upplysningar om hans besök på vissa webbplatser eller åtkomst av vissa filer på internet vid bestämda tidpunkter.

24 Det är emellertid inte möjligt att direkt fastställa Patrick Breyers identitet med hjälp av dessa lagrade uppgifter. De som driver de webbplatser som är aktuella i det nationella målet skulle nämligen endast kunna identifiera Patrick Breyer om hans internetleverantör gav dem uppgift om denna användares identitet. Frågan huruvida dessa uppgifter ska anses utgöra ”personuppgifter” beror följaktligen på huruvida Patrick Breyer är identifierbar.

25 Bundesgerichtshof (Federala högsta domstolen) har påpekat att det i doktrinen råder oenighet i frågan huruvida bedömningen av om en person är identifierbar ska ske utifrån ett ”objektivt” eller ett ”relativt” kriterium. En tillämpning av ett ”objektivt” kriterium skulle få till följd att det kunde anses att sådana uppgifter som de IP-adresser som är aktuella i det nationella målet, efter besök på de berörda webbplatserna, utgör personuppgifter även om endast en tredje man är i stånd att fastställa den berörda personens identitet, varvid denne tredje man i förevarande fall är Patrick Breyers internetleverantör som har lagrat ytterligare uppgifter vilka möjliggör identifiering av honom med hjälp av nämnda IP-adresser. Enligt ett ”relativt” kriterium skulle det kunna anses att sådana uppgifter utgör personuppgifter i förhållande till ett organ, såsom Patrick Breyers internetleverantör, eftersom de gör det möjligt att exakt identifiera användaren (se, för ett liknande resonemang, dom av den 24 november 2011, Scarlet Extended, C-70/10, EU:C:2011:771, punkt 51), men att de inte utgör personuppgifter i förhållande till ett annat organ, såsom det som driver de webbplatser som Patrick Breyer besökt, eftersom det organet, för det fall Patrick Breyer inte har uppgett sin identitet under besöken på webbplatserna, inte förfogar över de upplysningar som är nödvändiga för att utan överdriven ansträngning identifiera honom.

26 För det fall det ska anses att de dynamiska IP-adresserna till Patrick Breyers dator, tillsammans med en uppgift om datum för den session för vilken IP-adressen använts, utgör personuppgifter önskar den hänskjutande domstolen få klarlagt huruvida lagring av dessa IP-adresser efter denna session är tillåten enligt artikel 7 f i direktiv 95/46.

27 Bundesgerichtshof (Federala högsta domstolen) har i det avseendet preciserat att leverantörer av elektroniska informations- eller kommunikationstjänster, enligt 15 § stycke 1 TMG, endast får samla in och använda en användares personuppgifter i den mån det krävs för att möjliggöra och fakturera användningen av tjänsterna. Vidare har Bundesgerichtshof (Federala högsta domstolen) angett att lagring av nämnda uppgifter, enligt Förbundsrepubliken Tyskland, är nödvändig för att garantera säkerheten i de elektroniska informations- eller kommunikationstjänster som medlemsstaten håller tillgängliga för allmänheten via webbplatserna och säkerställa att webbplatserna fortsatt fungerar väl. Lagringen av uppgifterna gör det nämligen möjligt, i synnerhet, att identifiera så kallade överbelastningsattacker som genomförs i syfte att lamslå webbplatserna genom att vissa internetservrar överhopas av en stor mängd riktade och samordnade åtkomstansökningar och även att bekämpa sådana attacker.

28 I den mån det är nödvändigt att leverantören av elektroniska informations- eller kommunikationstjänster vidtar åtgärder för att bekämpa detta slags attacker skulle sådana åtgärder, enligt den hänskjutande domstolen, kunna anses vara nödvändiga för att ”möjliggöra … användningen av de elektroniska informations- eller kommunikationstjänsterna” med stöd av 15 § TMG. I doktrinen överväger dock uppfattningen, för det första, att insamling och användning av personuppgifter som rör en person som använder en webbplats endast är tillåtet för att möjliggöra en konkret session och, för det andra, att dessa uppgifter ska raderas efter sessionens slut, om de inte behövs för fakturering. En sådan restriktiv tolkning av 15 § stycke 1 TMG skulle emellertid utgöra hinder för att lagring av IP-adresser tillåts för att generellt garantera säkerheten i elektroniska informations- eller kommunikationstjänster och säkerställa att sådana tjänster fortsatt fungerar väl.

29 Den hänskjutande domstolen är osäker på huruvida den sistnämnda tolkningen, som är den tolkning som förespråkats av domstolen i andra instans, är i överensstämmelse med artikel 7 f i direktiv 95/46, med beaktande särskilt av de kriterier som EU-domstolen har slagit fast i punkt 29 och följande punkter i dom av den 24 november 2011, ASNEF och FECEMD (C-468/10 och C-469/10, EU:C:2011:777).

30 Mot denna bakgrund beslutade Bundesgerichtshof (Federala högsta domstolen) att vilandeförklara målet och ställa följande frågor till EU-domstolen:

”1) Ska artikel 2 a i direktiv 95/46 tolkas så, att en IP-adress som en leverantör [av elektroniska informations- eller kommunikationstjänster] registrerar i samband med att någon använder tjänsteleverantörens webbplats utgör en personuppgift för denne även om det är en tredje man (i förevarande fall internetleverantören) som förfogar över de ytterligare upplysningar som är nödvändiga för att identifiera den registrerade?

2) Utgör artikel 7 f i [nämnda direktiv] hinder för en nationell bestämmelse enligt vilken en leverantör av [elektroniska informations- eller kommunikationstjänster] endast får samla in och använda personuppgifter avseende en användare utan dennes samtycke i den mån det krävs för att möjliggöra och fakturera den aktuella användarens konkreta användning av tjänsten, och enligt vilken syftet att säkerställa den elektroniska informations- eller kommunikationstjänstens allmänna funktion inte kan rättfärdiga en användning av dessa uppgifter efter det att den aktuella sessionen har avslutats?”

Prövning av tolkningsfrågorna

Den första frågan

31 Den hänskjutande domstolen har ställt den första frågan för att få klarhet i huruvida artikel 2 a i direktiv 95/46 ska tolkas så, att en dynamisk IP-adress som en leverantör av elektroniska informations- eller kommunikationstjänster registrerar i samband med att en person besöker en webbplats som nämnda leverantör gör tillgänglig för allmänheten utgör en personuppgift i den mening som avses i nämnda bestämmelse i förhållande till leverantören, när endast en tredje man (i förevarande fall personens internetleverantör) förfogar över de ytterligare upplysningar som är nödvändiga för att identifiera personen.

32 Enligt nämnda bestämmelse avses med ”personuppgifter” ”varje upplysning som avser en identifierad eller identifierbar fysisk person (den registrerade)”. I samma bestämmelse anges att en identifierbar person är en person som kan identifieras, direkt eller indirekt, framför allt genom hänvisning till ett identifikationsnummer eller till en eller flera faktorer som är specifika för hans fysiska, fysiologiska, psykiska, ekonomiska, kulturella eller sociala identitet.

33 Det ska inledningsvis påpekas att EU-domstolen i punkt 51 i dom av den 24 november 2011, Scarlet Extended (C-70/10, EU:C:2011:771), vilken särskilt rörde tolkningen av direktiv 95/46, angav att internetanvändares IP-adresser utgör skyddade personuppgifter, eftersom de gör det möjligt att exakt identifiera dessa användare.

34 Domstolens uttalande i den domen rörde emellertid den situationen där det är internetleverantören som samlar in och identifierar internetanvändarnas IP-adresser.

35 I förevarande mål rör den första frågan den situationen där det är leverantören av elektroniska informations- eller kommunikationstjänster, det vill säga Förbundsrepubliken Tyskland, som registrerar IP-adresserna tillhörande de personer som använder en webbplats som denna tjänsteleverantör gör tillgänglig för allmänheten, varvid leverantören inte förfogar över de ytterligare upplysningar som är nödvändiga för att identifiera användarna.

36 Det är dessutom utrett att de IP-adresser som den hänskjutande domstolen hänvisar till är så kallade dynamiska IP-adresser, det vill säga tillfälliga IP-adresser som tilldelas vid varje uppkoppling till internet och som ersätts med nya adresser vid senare uppkopplingstillfällen, och inte så kallade statiska IP-adresser som inte förändras och som gör det möjligt att varaktigt identifiera den utrustning som är ansluten till internet.

37 Den första tolkningsfrågan bygger således på antagandet, för det första, att uppgifter som består av en dynamisk IP-adress samt datum och klockslag för sessionen då en webbplats besöktes från nämnda IP-adress och som registrerats av en leverantör av elektroniska informations- eller kommunikationstjänster inte i sig möjliggör för denna leverantör att identifiera den användare som besökte webbplatsen under den aktuella sessionen och, för det andra, att internetleverantören för sin del förfogar över ytterligare upplysningar, vilka – om de kopplades samman med denna IP-adress – skulle göra det möjligt att identifiera nämnda användare.

38 I detta avseende ska det påpekas att en dynamisk IP-adress inte utgör en upplysning som avser en ”identifierad fysisk person”, i och med att en sådan adress inte direkt röjer identiteten på den fysiska person som äger den dator från vilken en webbplats har besökts och inte heller identiteten på en annan person som skulle kunna använda den datorn.

39 I syfte att fastställa huruvida en dynamisk IP-adress, i den situation som beskrivits i punkt 37 ovan, utgör en personuppgift i den mening som avses i artikel 2 a i direktiv 95/46 i förhållande till en leverantör av elektroniska informations- eller kommunikationstjänster ska det vidare undersökas huruvida en sådan IP-adress, som registreras av en sådan tjänsteleverantör, kan anses utgöra en upplysning som avser en ”identifierad fysisk person”, när de ytterligare upplysningar som är nödvändiga för att identifiera användaren av en webbplats som denna tjänsteleverantör gör tillgänglig för allmänheten innehas av samma användares internetleverantör.

40 Av artikel 2 a i direktiv 95/46 framgår att en identifierbar person är en person som inte endast kan identifieras direkt utan även indirekt.

41 Unionslagstiftarens användning av ordet ”indirekt” tyder på att det inte är nödvändigt att upplysningen i sig gör det möjligt att identifiera den aktuella personen för att upplysningen ska anses utgöra en personuppgift.

42 I skäl 26 i direktiv 95/46 anges dessutom att man, för att avgöra om en person är identifierbar, ska beakta alla hjälpmedel som i syfte att identifiera vederbörande rimligen kan komma att användas antingen av den registeransvarige eller av någon annan person.

43 I nämnda skäl hänvisas till alla hjälpmedel som rimligen kan komma att användas antingen av den registeransvarige eller av någon ”annan person”. Ordalydelsen i det skälet antyder därigenom att det inte krävs att en enda person innehar alla upplysningar som är nödvändiga för att identifiera den aktuella personen för att en uppgift ska anses utgöra en ”personuppgift” i den mening som avses i artikel 2 a i direktiv 95/46.

44 Den omständigheten att de ytterligare upplysningar som är nödvändiga för att identifiera en användare av en webbplats inte innehas av leverantören av elektroniska informations- eller kommunikationstjänster, utan av användarens internetleverantör, utesluter således inte att de dynamiska IP-adresser som leverantören av elektroniska informations- eller kommunikationstjänster har registrerat utgör personuppgifter i den mening som avses i artikel 2 a i direktiv 95/46 för denne.

45 Det ska emellertid fastställas huruvida möjligheten att kombinera en dynamisk IP-adress med nämnda ytterligare information som internetleverantören innehar utgör ett hjälpmedel som rimligen kan komma att användas för att identifiera den aktuella personen.

46 Såsom generaladvokaten angav i punkt 68 i sitt förslag till avgörande skulle detta inte vara fallet om identifiering av den aktuella personen var förbjuden i lag eller omöjlig att genomföra i praktiken, exempelvis på grund av att den skulle kräva orimliga resurser i form av tid, kostnader och arbetskraft, med den följden att risken för identifiering i praktiken var försumbar.

47 Den hänskjutande domstolen har i begäran om förhandsavgörande preciserat att tysk rätt inte tillåter att internetleverantören överför de ytterligare upplysningar som är nödvändiga för att identifiera den aktuella personen direkt till leverantören av elektroniska informations- eller kommunikationstjänster. Det förefaller emellertid – med förbehåll för den undersökning härvidlag som det ankommer på den hänskjutande domstolen att göra – som om det finns lagliga medel som gör det möjligt för leverantören av elektroniska informations- eller kommunikationstjänster att, särskilt i händelse av it-attacker, vända sig till den behöriga myndigheten för att den ska vidta nödvändiga åtgärder för att erhålla sådana upplysningar från internetleverantören och inleda straffrättsliga förfaranden.

48 Det förefaller sålunda som om en leverantör av elektroniska informations- eller kommunikationstjänster förfogar över hjälpmedel som rimligen kan komma att användas för att med hjälp av andra personer – närmare bestämt den behöriga myndigheten och internetleverantören – identifiera den registrerade på grundval av de lagrade IP-adresserna.

49 Mot bakgrund av det ovan anförda ska den första tolkningsfrågan besvaras enligt följande. Artikel 2 a i direktiv 95/46 ska tolkas så, att en dynamisk IP-adress som en leverantör av elektroniska informations- eller kommunikationstjänster registrerar i samband med att en person besöker en webbplats som nämnda leverantör gör tillgänglig för allmänheten utgör en personuppgift i den mening som avses i nämnda bestämmelse i förhållande till leverantören, när denne förfogar över lagliga medel som gör det möjligt för vederbörande att identifiera den registrerade med hjälp av de ytterligare upplysningar som den registrerades internetleverantör förfogar över.

Den andra frågan

50 Den hänskjutande domstolen har ställt den andra frågan för att få klarhet i huruvida artikel 7 f i direktiv 95/46 ska tolkas så, att den utgör hinder för en medlemsstats bestämmelser enligt vilka en leverantör av elektroniska informations- eller kommunikationstjänster får samla in och använda personuppgifter avseende en användare av dessa tjänster utan dennes samtycke endast i den mån insamlingen och användningen krävs för att möjliggöra och fakturera den aktuella användarens konkreta användning av dessa tjänster, utan att syftet att säkerställa tjänsternas allmänna funktion kan rättfärdiga en användning av uppgifterna efter det att en session har avslutats.

51 Innan denna fråga besvaras ska det undersökas huruvida behandlingen av de i det nationella målet aktuella personuppgifterna, det vill säga de dynamiska IP-adresser som tillhör användarna av vissa webbplatser som drivs av tyska federala myndigheter, inte är undantagen från tillämpningsområdet för direktiv 95/46 enligt artikel 3.2 första strecksatsen däri. I den bestämmelsen föreskrivs att direktivet inte gäller för sådan behandling av personuppgifter som rör, bland annat, statens verksamhet på straffrättens område.

52 Det ska erinras om att den verksamhet som anges som exempel i nämnda bestämmelse i samtliga fall avser sådan verksamhet som endast kan bedrivas av staten eller statliga myndigheter och inte kan bedrivas av enskilda personer (se dom av den 6 november 2003, Lindqvist, C-101/01, EU:C:2003:596, punkt 43, och dom av den 16 december 2008, Satakunnan Markkinapörssi och Satamedia, C-73/07, EU:C:2008:727, punkt 41).

53 I det nationella målet förefaller det emellertid – med förbehåll för den undersökning härvidlag som det ankommer på den hänskjutande domstolen att göra – som om de tyska federala myndigheterna, vilka tillhandahåller elektroniska informations- eller kommunikationstjänster och vilka ansvarar för behandlingen av dynamiska IP-adresser, trots att de har ställning som offentliga myndigheter, agerar i egenskap av enskilda rättssubjekt och utanför statens verksamhet på straffrättens område.

54 Således ska det fastställas huruvida sådana nationella bestämmelser som de som är aktuella i förevarande mål är förenliga med artikel 7 f i direktiv 95/46.

55 De aktuella nationella bestämmelserna tillåter, enligt den restriktiva tolkning som den hänskjutande domstolen har hänvisat till, insamling och användning av personuppgifter avseende en användare av nämnda tjänster utan dennes samtycke endast i den mån detta krävs för att möjliggöra och fakturera den aktuella användarens konkreta användning av tjänsten, utan att syftet att säkerställa de elektroniska informations- eller kommunikationstjänsternas allmänna funktion kan rättfärdiga en användning av uppgifterna efter det att den aktuella sessionen har avslutats.

56 Enligt artikel 7 f i direktiv 95/46 är behandling av personuppgifter tillåten om behandlingen är ”nödvändig för ändamål som rör berättigade intressen hos den registeransvarige eller hos den eller de tredje män till vilka uppgifterna har lämnats ut, utom när sådana intressen uppvägs av den registrerades intressen eller dennes grundläggande fri- och rättigheter som kräver skydd under artikel 1.1” i direktivet.

57 Domstolen har slagit fast att det i artikel 7 i direktiv 95/46 görs en uttömmande uppräkning av de situationer där en behandling av personuppgifter kan anses vara tillåten och att medlemsstaterna varken får foga ytterligare principer för tillåtligheten av behandlingen av personuppgifter till dem som nämns i den artikeln eller föreskriva ytterligare villkor som påverkar räckvidden av de sex principer som föreskrivs däri (se, för ett liknande resonemang, dom av den 24 november 2011, ASNEF och FECEMD, C-468/10 och C-469/10, EU:C:2011:777, punkterna 30 och 32).

58 Medlemsstaterna har visserligen enligt artikel 5 i direktiv 95/46 rätt att inom de begränsningar som bestämmelserna i kapitel II – och följaktligen artikel 7 – innebär precisera på vilka villkor behandling av personuppgifter är tillåten. Medlemsstaterna får emellertid endast använda det handlingsutrymme de har enligt nämnda artikel 5 i överensstämmelse med direktivets syfte, nämligen att upprätthålla en balans mellan det fria flödet av personuppgifter och skyddet för privatlivet. Medlemsstaterna får inte heller, på grundval av artikel 5 i direktivet, införa ytterligare principer för tillåtligheten av behandlingen av personuppgifter utöver dem som nämns i artikel 7 i direktivet eller föreskriva ytterligare villkor som påverkar räckvidden av de sex principer som föreskrivs i artikel 7 (se, för ett liknande resonemang, dom av den 24 november 2011, ASNEF och FECEMD, C-468/10 och C-469/10, EU:C:2011:777, punkterna 33, 34 och 36).

59 Om 15 § TMG tolkades på det restriktiva sätt som anges i punkt 55 ovan skulle den bestämmelsen ha en mer begränsad räckvidd än den princip som föreskrivs i artikel 7 f i direktiv 95/46.

60 I artikel 7 f i direktivet hänvisas nämligen allmänt till uppnåendet av ”ändamål som rör berättigade intressen hos den registeransvarige eller hos den eller de tredje män till vilka uppgifterna har lämnats ut”, medan tjänsteleverantören enligt 15 § TMG endast får samla in och använda personuppgifter avseende en användare i den mån det krävs för att möjliggöra och fakturera den konkreta användningen av den elektroniska informations- eller kommunikationstjänsten. Således utgör 15 § TMG rent allmänt hinder mot att personuppgifter lagras efter en session för användning av elektroniska informations- eller kommunikationstjänster i syfte att garantera tillgången till tjänsterna. De tyska federala myndigheter som tillhandahåller elektroniska informations- eller kommunikationstjänster skulle emellertid också kunna ha ett berättigat intresse av att, utöver varje konkret användning av deras respektive allmänt tillgängliga webbplatser, säkerställa att webbplatserna fortsatt fungerar väl.

61 Såsom generaladvokaten har angett i punkterna 100 och 101 i sitt förslag till avgörande begränsar sig inte en sådan nationell bestämmelse till att, i enlighet med vad som föreskrivs i artikel 5 i direktiv 95/46, precisera begreppet berättigade intressen i artikel 7 f i det direktivet.

62 Det ska härvid även erinras om att artikel 7 f i direktivet utgör hinder för att en medlemsstat kategoriskt och generellt utesluter möjligheten att behandla vissa typer av personuppgifter, utan att tillåta en avvägning mellan de motstående rättigheterna och intressena i det enskilda fallet. En medlemsstat får sålunda inte, för dessa typer av personuppgifter, slutgiltigt ange vad resultatet av avvägningen mellan de motstående rättigheterna och intressena blir, utan att tillåta ett annat resultat med hänsyn till de särskilda omständigheterna i det enskilda fallet (se, för ett liknande resonemang, dom av den 24 november 2011, ASNEF och FECEMD, C-468/10 och C-469/10, EU:C:2011:777, punkterna 47 och 48).

63 Sådana nationella bestämmelser som de nu aktuella begränsar emellertid, med avseende på behandlingen av personuppgifter avseende användare av webbplatser för elektroniska informations- eller kommunikationstjänster, räckvidden för den princip som föreskrivs i artikel 7 f i direktiv 95/46 genom att det inte är tillåtet att syftet att säkerställa de elektroniska informations- eller kommunikationstjänsternas allmänna funktion vägs mot användarnas intressen eller grundläggande rättigheter och friheter, vilka enligt artikel 1.1 i direktivet ska skyddas.

64 Det följer av det ovan anförda att den andra frågan ska besvaras enligt följande. Artikel 7 f i direktiv 95/46 ska tolkas så, att den utgör hinder för en medlemsstats bestämmelser enligt vilka en leverantör av elektroniska informations- eller kommunikationstjänster får samla in och använda personuppgifter avseende en användare av dessa tjänster utan dennes samtycke endast i den mån insamlingen och användningen krävs för att möjliggöra och fakturera den aktuella användarens konkreta användning av dessa tjänster, utan att syftet att säkerställa tjänsternas allmänna funktion kan rättfärdiga en användning av uppgifterna efter det att en session har avslutats.

Rättegångskostnader

65 Eftersom förfarandet i förhållande till parterna i det nationella målet utgör ett led i beredningen av samma mål, ankommer det på den hänskjutande domstolen att besluta om rättegångskostnaderna. De kostnader för att avge yttrande till domstolen som andra än nämnda parter har haft är inte ersättningsgilla.

Mot denna bakgrund beslutar domstolen (andra avdelningen) följande:

1) **Artikel 2 a i Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter ska tolkas så, att en dynamisk IP-adress som en leverantör av elektroniska informations- eller kommunikationstjänster registrerar i samband med att en person besöker en webbplats som nämnda leverantör gör tillgänglig för allmänheten utgör en personuppgift i den mening som avses i nämnda bestämmelse i förhållande till leverantören, när denne förfogar över lagliga medel som gör det möjligt för vederbörande att identifiera den registrerade med hjälp av de ytterligare upplysningar som den registrerades internetleverantör förfogar över.**

2) **Artikel 7 f i direktiv 95/46 ska tolkas så, att den utgör hinder för en medlemsstats bestämmelser enligt vilka en leverantör av elektroniska informations- eller kommunikationstjänster får samla in och använda personuppgifter avseende en användare av dessa tjänster utan dennes samtycke endast i den mån insamlingen och användningen krävs för att möjliggöra och fakturera den aktuella användarens konkreta användning av dessa tjänster, utan att syftet att säkerställa tjänsternas allmänna funktion kan rättfärdiga en användning av uppgifterna efter det att en session har avslutats.**

Underskrifter