Rättsfallssamlingen

FÖRSLAG TILL AVGÖRANDE AV GENERALADVOKAT
MANUEL CAMPOS SÁNCHEZ-BORDONA
föredraget den 12 maj 2016 [1]

Mål C-582/14

Patrick Breyer
mot
Bundesrepublik Deutschland

(Begäran om förhandsavgörande från Bundesgerichtshof (Federala högsta domstolen i Tyskland)

”Behandling av personuppgifter — Direktiv 95/46/EG — Artikel 2 a och artikel 7 f — Begreppet personuppgifter — IP-adresser — Lagring som görs av en leverantör av elektroniska medietjänster — Nationell lagstiftning som inte gör det möjligt att beakta den registeransvariges berättigade intresse”

1. En IP-adress är en siffersträng som tilldelas en enhet (en dator, en datorplatta, en smarttelefon), identifierar den och gör det möjligt för den att få tillgång till det elektroniska kommunikationsnätet. För att enheten ska kunna anslutas till internet, måste den siffersträng som tillhandahålls av internetleverantören användas. IP-adressen överförs till den server på vilken den aktuella webbplatsen är lagrad.

2. I synnerhet tilldelar internetleverantörerna (vanligtvis telefonbolag) sina kunder tillfälliga, så kallade dynamiska IP-adresser för varje anslutning till internet och dessa adresser ändras vid senare anslutningar. Samma bolag för register över vilken IP-adress som har tilldelats en viss enhet vid ett visst tillfälle. [2]

3. Innehavarna av de webbplatser som man får tillgång till med hjälp av de dynamiska IP-adresserna brukar också föra register över vilka sidor som har använts, samt när det skedde och från vilken dynamisk IP-adress. Dessa register får, tekniskt sett, lagras utan tidsbegränsning, efter det att användarens anslutning till internet har avslutats.

4. Enbart en dynamisk IP-adress räcker inte för att tjänsteleverantören ska kunna identifiera den som använder hans webbplats. Han kan emellertid göra det om han kombinerar den dynamiska IP-adressen med andra uppgifter som internetleverantören förfogar över.

1 — Originalspråk: spanska.

2 — I artikel 5 i Europaparlamentets och rådets direktiv 2006/24/EG av den 15 mars 2006 om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG (EUT 2006, L 105, s. 54) föreskrevs olika skyldigheter för att kunna utreda, avslöja och åtala brott, bland annat att lagra ”datum och tid för på- respektive avloggning i Internetåtkomsttjänsten ... Tillsammans med IP-adressen, oavsett om den är dynamisk eller statisk, som en kommunikation tilldelats av Internetåtkomstleverantören till en kommunikation och abonnents eller registrerad användares användar-ID”.

5. I förevarande mål är det omtvistat huruvida de dynamiska IP-adresserna utgör personuppgifter i den mening som avses i artikel 2 a i direktiv 95/46/EG.[3] För att kunna besvara denna fråga måste det först fastställas vilken betydelse det i detta sammanhang har att det inte är innehavaren av webbplatsen som förfogar över de ytterligare uppgifter som krävs för att identifiera användaren utan en tredje man (närmare bestämt internetleverantören).

6. Detta är en fråga som domstolen inte tidigare har prövat. I punkt 51 i domen i målet Scarlet Extended[4] slog domstolen visserligen fast att IP-adresser ”utgör skyddade personuppgifter eftersom de gör det möjligt att exakt identifiera användarna”, men det gällde ett sammanhang där IP-adresserna samlades in och identifierades av internetleverantören[5] och inte av en innehållsleverantör, som i förevarande fall.

7. Skulle de dynamiska IP-adresserna utgöra personuppgifter för tjänsteleverantören, behöver det därefter prövas huruvida behandlingen av dem omfattas av tillämpningsområdet för direktiv 95/46.

8. Även om de skulle utgöra personuppgifter är det inte säkert att de åtnjuter det skydd som följer av direktiv 95/46, till exempel om syftet med behandlingen av dem är att vidta straffrättsliga åtgärder mot personer som utsätter webbplatsen för angrepp. I det fallet är direktiv 95/46 inte tillämpligt, enligt artikel 3.2 första strecksatsen.

9. Det måste dessutom klargöras huruvida tjänsteleverantören som registrerar de dynamiska IP-adresserna när användaren går in på dennes webbplatser (i det här fallet Bundesrepublik Deutschland), handlar i egenskap av offentlig myndighet eller i egenskap av enskild.

10. Om direktiv 95/46 är tillämpligt måste det avslutningsvis klargöras i vilken mån nationella bestämmelser, som inskränker räckvidden av ett av de villkor som fastställs i direktivet för att motivera behandlingen av personuppgifter, är förenliga med artikel 7 f i direktivet.

I – Tillämpliga bestämmelser

A – *Unionsrätt*

11. Skäl 26 i direktiv 95/46 har följande lydelse:

”(26) 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.”

12. I artikel 1 i direktiv 95/46 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.

3 — 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 1995, L 281, s. 31).

4 — Dom av den 24 november 2011 (C-70/10, EU:C:2011:771), punkt 51.

5 — Så skedde även i dom av den 19 april 2012, Bonnier Audio m.fl. (C-461/10, EU:C:2012:219), punkterna 51 och 52.

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.”

13. Artikel 2 i direktiv 95/46 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) : 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*: den fysiska eller juridiska person, den myndighet, den institution eller det andra organ än den registrerade, den registeransvarige, registerföraren och de personer som under den registeransvariges eller registerförarens direkta ansvar har befogenhet att behandla uppgifterna,

…”

14. Under rubriken ”Tillämpningsområde” föreskrivs följande i artikel 3 i direktiv 95/46:

”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,

…”

15. Kapitel II i direktiv 95/46, vilket handlar om ”Allmänna bestämmelser om när personuppgifter får behandlas”, inleds med artikel 5, som har följande lydelse: ”Medlemsstaterna skall inom de begränsningar som bestämmelserna i detta kapitel innebär, precisera på vilka villkor behandling av personuppgifter är tillåten.”

16. I artikel 6 i direktiv 95/46 föreskrivs följande:

”1. Medlemsstaterna skall föreskriva att personuppgifter

a) skall behandlas på ett korrekt och lagligt sätt,

b) skall samlas in för särskilda, uttryckligt angivna och berättigade ändamål; senare behandling får inte ske på ett sätt som är oförenligt med dessa ändamål. Senare behandling av uppgifter för historiska, statistiska eller vetenskapliga ändamål skall inte anses oförenlig med dessa ändamål förutsatt att medlemsstaterna beslutar om lämpliga skyddsåtgärder,

c) skall vara adekvata och relevanta och inte får omfatta mer än vad som är nödvändigt med hänsyn till de ändamål för vilka de har samlats in och för vilka de senare behandlas,

d) skall vara riktiga och, om nödvändigt, aktuella. Alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga eller ofullständiga i förhållande till de ändamål för vilka de samlades in eller för vilka de senare behandlas, utplånas eller rättas,

e) förvaras på ett sätt som förhindrar identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka uppgifterna samlades in eller för vilka de senare behandlades. Medlemsstaterna skall vidta lämpliga skyddsåtgärder för de personuppgifter som lagras under längre perioder för historiska, statistiska eller vetenskapliga ändamål.

2. Det åligger den registeransvarige att säkerställa att punkt 1 efterlevs.”

17. Artikel 7 i direktiv 95/46 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, eller

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.”

18. I artikel 13 i direktiv 95/46 föreskrivs följande:

”1. 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

a) statens säkerhet,

b) försvaret,

c) allmän säkerhet,

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

e) ett viktigt ekonomiskt eller finansiellt intresse hos en medlemsstat eller hos Europeiska unionen, inklusive monetära frågor, budgetfrågor och skattefrågor,

f) en tillsyns-, inspektions- eller regleringsfunktion som, även om den är av övergående karaktär, är förbunden med myndighetsutövning i de under punkterna c), d) och e) nämnda fallen,

g) skydd av den registrerades eller andras fri- och rättigheter.

…”

B – *Nationell rätt*

19. I 12 § teletjänstlagen (Telemediengesetz, nedan kallad TMG) [6] föreskrivs följande:

”1. Vid tillhandahållandet av teletjänster får tjänsteleverantören endast insamla och behandla personuppgifter om detta uttryckligen är tillåtet enligt denna lag eller en annan lag som uttryckligen avser teletjänster, eller om användaren har gett sitt samtycke.

2. De personuppgifter som insamlats för att tillhandahålla teletjänster får tjänsteleverantören endast använda i andra syften såvitt detta uttryckligen är tillåtet enligt denna lag eller en annan lag som uttryckligen avser teletjänster, eller om användaren har gett sitt samtycke.

3. Om ej annat föreskrivs ska de gällande bestämmelserna om skydd för personuppgifter tillämpas även när uppgifterna inte behandlas genom automatisk databehandling.”

20. 15 § TMG har följande lydelse:

”1. Tjänsteleverantören får endast insamla och använda en användares personuppgifter i den mån detta krävs för att möjliggöra användningen av teletjänsten samt faktureringen för detta (användningsdata). Användningsdata är bland annat

1) uppgifter för att identifiera användaren,

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

3) uppgifter om de teletjänster som användaren använt.

2. Tjänsteleverantören får sammanföra en användares användningsdata i den mån detta behövs för faktureringen av användaren.

…

6 — Lag av den 26 februari 2007 (BGBl 2007 I, s. 179).

4. Tjänsteleverantören får använda användningsdata efter det att sessionen avslutats i den mån detta krävs för fakturering av användaren (faktureringsdata). Tjänsteleverantören kan låsa dessa data för att uppfylla krav i lagar, förordningar eller avtal. ...”

21. I 3 § punkt 1 dataskyddslagen (Bundesdatenschutzgesetz nedan kallad BDSG),[7] föreskrivs att ”[p]ersonuppgifter är uppgifter angående personliga eller faktiska omständigheter avseende en identifierad eller identifierbar fysisk person (den registrerade personen). ...”

II – Faktiska omständigheter

22. Patrick Breyer har väckt talan mot Bundesrepublik Deutschland med yrkande om förbudsföreläggande avseende lagring av IP-adresser.

23. Många tyska offentliga institutioner driver allmänt tillgängliga webbplatser genom vilka de tillhandahåller aktuell information. I syfte att avvärja attacker och möjliggöra lagföring av angripare, lagras för de flesta av dess webbplatser alla operationer för att erhålla tillgång i logfiler. Därvid lagras, även efter sessionens slut, namnet på de eftersökta uppgifterna respektive sidorna, de begrepp som angetts i sökfält, tidpunkten för åtkomsten, den överförda datamängden, uppgiften om huruvida försöket till åtkomst var framgångsrikt, och IP-adressen för den dator från vilken åtkomst söktes.

24. Patrick Breyer har förut gått in på olika sådana webbplatser. I sin ansökan yrkade han att motparten skulle föreläggas att avhålla sig från att lagra, eller låta tredje man lagra, IP-adressen för Patrick Breyers värdsystem, vilken överförs i samband med användningen av motpartens teletjänster, i den mån denna lagring inte var nödvändig för att vid störningar återupprätta möjligheten att förfoga över telemediet.

25. Domstolen i första instans ogillade Patrick Breyers talan. Efter det att Patrick Breyer överklagat denna dom ändrade appellationsdomstolen den delvis och förelade motparten att avhålla sig från att efter sessionens slut lagra IP-adressen. Förbudsföreläggandet gällde i den mån Patrick Breyer under sin session uppgett sin identitet, inbegripet via en e-postadress, och i den mån en sådan lagring inte krävs för återställande av förfogande över telemediet i störningsfall.

III – Tolkningsfrågor

26. Båda parterna har överklagat appellationsdomstolens dom och Bundesgerichtshofs (Federala högsta domstolen i Tyskland) sjätte avdelning har den 17 december 2014 hänskjutit följande tolkningsfrågor:

”1) Ska artikel 2 a i ... direktiv 95/46/EG … tolkas så, att en IP-adress som en tjänsteleverantör lagrar i samband med att någon använder tjänsteleverantörens webbplats utgör en personuppgift för denne redan när en tredje man (här: internetleverantören) förfogar över de ytterligare uppgifter som krävs för att identifiera den registrerade?

2) Utgör artikel 7 f i dataskyddsdirektivet hinder för en bestämmelse i nationell rätt enligt vilken en tjänsteleverantör endast kan samla in och använda personuppgifter för en användare utan dennes samtycke i den mån detta krävs för att möjliggöra, och ta betalt för, den aktuella användarens konkreta användning av teletjänsten och enligt vilken syftet att säkerställa teletjänstens allmänna funktion inte kan rättfärdiga en användning efter det att den aktuella sessionen har avslutats?”

7 — Lag av den 20 december 1990 (BGBl 1990 I, s. 2954).

27. Den hänskjutande domstolen har förklarat att klaganden enligt tysk rätt kunde kräva att motparten avstår från att lagra IP-adresserna, om lagringen enligt dataskyddslagstiftningen utgör ett rättsstridigt ingrepp i klagandens rätt till skydd av sin person, närmare bestämt hans rätt att ”själv bestämma över utlämnandet och användningen av personuppgifter” (1004 § punkt 1 och 823 § punkt 1 i den tyska civillagen (Bürgerliches Gesetzbuch), jämförda med artiklarna 1 och 2 i grundlagen (Grundgesetz)).

28. Detta är fallet om a) IP-adressen (under alla omständigheter kombinerad med tidpunkten för åtkomsten av en webbplats), ska anses utgöra en ”personuppgift” i den mening som avses i artikel 2 a i direktiv 95/46, jämförd med skäl 26 andra meningen i direktivet, eller 12 § punkterna 1 och 3 TMG, jämförd med 3 § 1 p BDSG, och om b) det inte föreligger någon tillåtelsegrund i enlighet med artikel 7 f i direktiv 95/46 och 12 § punkterna 1 och 3 samt 15 § punkterna 1 och 4 TMG.

29. Enligt Bundesgerichtshof är det för att tolka den nationella rätten (12 § punkt 1 TMG) nödvändigt att få reda på hur begreppet personuppgifter i artikel 2 a i direktiv 95/46 ska tolkas.

30. Dessutom har den hänskjutande domstolen påpekat att eftersom tjänsteleverantören enligt 15 § punkt 1 TMG endast får samla in och använda en användares personuppgifter i den mån detta krävs för att möjliggöra användningen av teletjänsten samt faktureringen för denna (användningsdata),[8] är tolkningen av den bestämmelsen kopplad till hur artikel 7 f i direktiv 95/46 ska tolkas.

IV – Förfarandet vid domstolen. Parternas argument

31. Den tyska, den österrikiska och den portugisiska regeringen, samt kommissionen har lämnat skriftliga yttranden. Endast kommissionen och Patrick Breyer närvarade vid förhandlingen den 25 februari 2016, i vilken den tyska regeringen avböjde att medverka.

A – *Parternas argument rörande den första tolkningsfrågan*

32. Personuppgifter är enligt Patrick Breyer även uppgifter som det bara är teoretiskt möjligt att kombinera, det vill säga där man utgår från en abstrakt potentiell fara och där det saknar betydelse huruvida en sådan kombination verkligen görs i praktiken. Att det är relativt svårt för ett organ att identifiera en person med hjälp av IP-adressen innebär inte, enligt Breyer, att det inte föreligger en fara för den personen. Dessutom menar Breyer att det är av betydelse att Tyskland lagrar sina IP-uppgifter för att, vid behov, kunna identifiera eventuella attacker eller lagföra dem, vilket är tillåtet enligt 113 § i Telekommunikationsgesetz (lagen om telekommunikation) och även har skett vid ett stort antal tillfällen.

33. Den tyska regeringen anser att den första frågan ska besvaras nekande. Enligt den tyska regeringen avslöjar en dynamisk IP-adress inte en ”identifierad” person, i den mening som avses i artikel 2 a i direktiv 95/46/EG. För att avgöra om IP-adressen ger information om en ”identifierbar” person, i den mening som avses i samma artikel, ska identifierbarhetsprövningen göras med hjälp av ett ”relativt” kriterium. Detta följer enligt den tyska regeringen av skäl 26 i direktiv 95/46, enligt vilket endast de hjälpmedel som i syfte att identifiera en person ”rimligen” kan komma att användas antingen av den registeransvarige eller av någon annan person, ska beaktas. Denna precisering tyder enligt den tyska regeringen på att unionslagstiftaren inte har velat att situationer där en identifiering är objektivt möjlig för vilken tredje man som helst, ska omfattas av direktivets tillämpningsområde.

8 — Enligt Bundesgerichtshof är användningsdata uppgifter för att identifiera användaren, uppgifter om när den aktuella användningen inleddes och avslutades, samt dess omfattning och uppgifter om de teletjänster som användaren använt.

34. Den tyska regeringen anser också att begreppet ”personuppgifter”, i den mening som avses i artikel 2 a i direktiv 95/46, ska tolkas mot bakgrund av direktivets syfte, det vill säga att respekten för de grundläggande rättigheterna ska iakttas. Behovet av att skydda fysiska personer skulle kunna uppfattas på olika sätt beroende på vem som innehar uppgifterna och huruvida denne förfogar över medel för att använda sig av dem för att identifiera personerna.

35. Den tyska regeringen anser att Breyer inte är identifierbar med hjälp av IP-adresserna i kombination med andra uppgifter som innehållsleverantörerna förfogar över. För detta krävs enligt den tyska regeringen att man hanterar den information som internetleverantörerna förfogar över, vilka inte får vidarebefordra dem till innehållsleverantörerna, eftersom det saknas rättslig grund för det.

36. Den österrikiska regeringen anser däremot att frågan ska besvaras jakande. Av skäl 26 i direktiv 95/46 framgår att alla identifikationsuppgifter inte behöver finnas hos en och samma enhet för att en person ska anses vara identifierbar. Således skulle en IP-adress kunna utgöra en personuppgift om någon annan (till exempel internetleverantören) förfogar över medel för att identifiera innehavaren av den adressen, utan att det innebär orimliga ansträngningar.

37. Den portugisiska regeringen förespråkar också ett jakande svar. Den anser att IP-adressen, i kombination med tidpunkten för sessionen, utgör en personuppgift, eftersom den kan leda till att användaren identifieras av en annan enhet än den som har lagrat IP-adressen.

38. Kommissionen förespråkar också ett jakande svar och hänvisar till den lösning som domstolen valde i målet Scarlet Extended.[9] Kommissionen menar att eftersom lagringen av IP-adresser just syftar till att identifiera användarna vid it-angrepp, utgör de kompletterande uppgifter som internetleverantörerna lagrar ett hjälpmedel som ”rimligen” kan komma att användas, i den mening som avses i skäl 26 i direktiv 95/46. Med andra ord anser kommissionen att såväl syftet med direktivet som artiklarna 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna (nedan kallad stadgan) talar för att artikel 2 a i direktiv 95/46 ska ges en vid tolkning.

B – *Parternas argument rörande den andra tolkningsfrågan*

39. Patrick Breyer anser att artikel 7 f i direktiv 95/46 utgör en generalklausul som kräver precisering för att kunna tillämpas i praktiken. Enligt domstolens praxis handlar det således om att bedöma omständigheterna i det enskilda fallet och att avgöra om det finns grupper med berättigade intressen, i den mening som avses i den bestämmelsen, och det är inte bara tillåtet, utan nödvändigt att föreskriva särskilda regler för dessa grupper, för att tillämpa den artikeln. I detta fall, anser Breyer, är de nationella bestämmelserna förenliga med artikel 7 f i direktiv 95/46, eftersom den offentliga webbplatsen inte har något intresse av att lagra personuppgifter, eller på grund av att intresset av att skydda anonymiteten väger tyngre. Enligt Breyer är en systematisk och personlig lagring av uppgifterna emellertid inte förenlig med ett demokratiskt samhälle och inte heller nödvändig eller proportionerlig för att säkerställa de elektroniska mediernas funktionsduglighet, vilket är fullt möjligt utan att lagra dessa personuppgifter. Detta visar också vissa federala ministeriers webbplatser.

40. Den tyska regeringen anser att det saknas skäl att besvara den andra tolkningsfrågan, vilken enbart ställs om den första frågan ska besvaras jakande. Så är inte fallet enligt den tyska regeringen, av de ovan redovisade skälen.

41. Den österrikiska regeringen har föreslagit att frågan ska besvaras så, att direktiv 95/46 generellt sett inte utgör hinder för att uppgifter som de som är aktuella i det nationella målet lagras, när det är nödvändigt för att säkerställa att elektroniska medier fungerar väl. Enligt den österrikiska regeringen kan en begränsad lagring av IP-adressen, efter det att användningen av webbplatsen har avslutats, vara

9 — Dom av den 24 november 2011 (C-70/10, EU:C:2011:771), punkt 51.

rättsenlig vad beträffar skyldigheten för den registeransvarige att genomföra de åtgärder för att skydda dessa uppgifter som föreskrivs i artikel 17.1 i direktiv 95/46. Insatser mot it-attacker kan rättfärdiga en granskning av uppgifter rörande tidigare attacker och att vissa IP-adresser nekas tillträde till den aktuella webbplatsen. Frågan huruvida lagringen av uppgifter som dem som är aktuella i det nationella målet är proportionerlig, vad beträffar syftet att säkerställa att de elektroniska medierna fungerar väl, bör prövas i varje enskilt fall, med beaktande av de principer som anges i artikel 6.1 i direktiv 95/46.

42. Den portugisiska regeringen har gjort gällande att artikel 7 f i direktiv 95/46 inte utgör hinder för de nationella bestämmelser som är aktuella i det nationella målet, eftersom den tyska lagstiftaren redan har gjort en sådan avvägning som föreskrivs i den bestämmelsen, mellan den registeransvariges berättigade intressen å ena sidan, och den registrerades grundläggande fri- och rättigheter, å den andra.

43. Kommissionen anser att syftet med behandlingen av personuppgifter måste definieras på ett sådant sätt att det kan förutses av den berörda personen i de nationella bestämmelser genom vilka artikel 7 f i direktiv 95/46 införlivas. Enligt kommissionen uppfyller den tyska lagstiftningen inte detta krav, eftersom det i 15 § punkt 1 TMG föreskrivs att lagring av IP-adresser är tillåten ”när det är nödvändigt för att telekommunikationstjänsterna ska kunna användas”.

44. Kommissionen har således föreslagit att den andra tolkningsfrågan ska besvaras så, att denna bestämmelse utgör hinder för en tolkning av en nationell bestämmelse, enligt vilken en offentlig myndighet som handlar som en tjänsteleverantör får samla in och använda en användares personuppgifter utan dennes samtycke, även om syftet är att säkerställa att det elektroniska mediet fungerar väl generellt, om detta syfte inte tillräckligt tydligt och precist föreskrivs i den aktuella bestämmelsen.

V – Bedömning

A – *Den första tolkningsfrågan*

1. Avgränsning av tolkningsfrågan

45. Att döma av det sätt på vilket Bundesgerichtshof har formulerat den första tolkningsfrågan, är syftet med den att få klarlagt huruvida en IP-adress, med hjälp av vilken en webbplats kan användas, utgör en personuppgift (i den mening som avses i artikel 2 a i direktiv 95/46/EG) för det offentliga organ som är innehavare av webbplatsen, när internetleverantören förfogar över ytterligare uppgifter som gör det möjligt att identifiera den registrerade.

46. Formuleras frågan så, är den tillräckligt precis för att till att börja med utesluta andra abstrakta frågor som skulle kunna uppkomma rörande IP-adressernas rättsliga karaktär i samband med skydd av personuppgifter.

47. För det första har Bundesgerichtshof endast hänvisat till ”dynamiska IP-adresser”, det vill säga adresser som tilldelas tillfälligt för varje anslutning till internet och som ändras vid senare anslutningar. De utgör således inte ”fasta eller statiska IP-adresser”, vilka karaktäriseras av att de är oföränderliga och gör det möjligt att permanent identifiera den enhet som är ansluten till nätet.

48. För det andra utgår den hänskjutande domstolen från antagandet att tjänsteleverantören i det nationella målet inte med hjälp av den dynamiska IP-adressen kan identifiera dem som besöker dess sidor och inte heller själv förfogar över ytterligare uppgifter som i kombination med IP-adressen möjliggör en identifiering av dem. Bundesgerichtshof tycks i det sammanhanget anse att den dynamiska IP-adressen inte utgör en personuppgift, i den mening som avses i artikel 2 a i direktiv 95/46, *för tjänsteleverantören*.

49. Den hänskjutande domstolens fråga hänger samman med möjligheten att den dynamiska IP-adressen anses vara en personuppgift för tjänsteleverantören *när en tredje man förfogar över ytterligare uppgifter* som i kombination med IP-adressen kan identifiera den som använder webbplatsen. Bundesgerichtshof syftar emellertid inte på vilken tredje man som helst som förfogar över de ytterligare uppgifterna, utan enbart på internetleverantören (vilket innebär att den utesluter andra möjliga innehavare av den här typen av uppgifter), och detta är ytterligare en precisering av intresse.

50. Således är bland annat följande aspekter inte föremål för tvisten: a) huruvida statiska IP-adresser utgör personuppgifter enligt direktiv 95/46,[10] b) huruvida dynamiska IP-adresser, alltid och under alla förhållanden, är personuppgifter i den mening som avses i direktivet, samt avslutningsvis c) huruvida det är oundvikligt att de dynamiska IP-adresserna betecknas som personuppgifter när det finns en tredje man, oavsett vem det är, som kan använda dem för att identifiera nätanvändarna.

51. Det handlar således enbart om att avgöra huruvida en dynamisk IP-adress utgör en personuppgift för en tjänstleverantör när det kommunikationsföretag som erbjuder tillgång till nätet (internetleverantören) hanterar ytterligare uppgifter som, i kombination med IP-adressen, gör det möjligt att identifiera den som använder webbplatsen som handhas av den förstnämnda parten.

2. Prövning i sak

52. Den fråga som aktualiseras i förevarande mål om förhandsavgörande är föremål för en intensiv debatt i tysk doktrin och rättspraxis och debatten har polariserats i två åsiktsströmningar.[11] Enligt den ena (som utgår från ett ”objektivt” eller ”absolut” kriterium) är en användare identifierbar – och således är IP-adressen en personuppgift som kan ges skydd – när denne kan identifieras, oavsett vilka hjälpmedel och vilken kompetens som tjänsteleverantören har, enbart genom att kombinera den dynamiska IP-adressen med de uppgifter som tillhandahålls av en tredje man (exempelvis internetleverantören).

53. För anhängarna av den andra strömningen (vilka utgår från ett ”relativt” kriterium), räcker det inte att det finns en möjlighet att få hjälp av en tredje man med den slutliga identifieringen av användaren för att den dynamiska IP-adressen ska anses utgöra en personuppgift. Det viktiga är att den som har tillgång till uppgiften kan använda sig av den, med sina egna hjälpmedel, och på så sätt identifiera en person.

10 — Ett problem som behandlats av domstolen i domarna av den 24 november 2011, Scarlet Extended (C-70/10, EU:C:2011:771), punkt 51, och av den 19 april 2012, Bonnier Audio m.fl. (C-461/10, EU:C:2012:219). I punkterna 51 och 52 i den sistnämnda domen drog domstolen slutsatsen att tillhandahållande av ”information om namn på och adress till en ... internetanvändare som använt sig av den IP-adress som antas ha använts för olaglig fildelning av filer innehållande skyddade verk, detta i syfte att kunna identifiera denna person. … utgör behandling av personuppgifter i den mening som avses i artikel 2 första stycket i direktiv 2002/58 jämförd med artikel 2 b i direktiv 95/46”.

11 — Beträffande de båda ståndpunkterna i doktrinen, se Schreibauer, M., i *Kommentar zum Bundesdatenschutzgesetz. Nebengesetze*, Esser, M., Kramer, P., och von Lewinski, K. (red.), Carl Heymanns Verlag/Wolters Kluwer, Köln, 2014, 4 uppl., § 11 Telemediengesetz (4–10). Nink, J., och Pohle, J.: ”Die Bestimmbarkeit des Personenbezugs. Von der IP-Adresse zum Anwendungsbereich der Datenschutzgesetze”, i *Multimedia und Recht*, 9/2015, sidorna 563–567. Heidrich, J. och Wegener, C.: ”Rechtliche und technische Anforderungen an die Protokollierung von IT-Daten. Problemfall Logging”, i *Multimedia und Recht*, 8/2015, sidorna 487–492. Leisterer, H.: ”Die neuen Pflichten zur Netz– und Informationssicherheit und die Verarbeitung personenbezogener Daten zur Gefahrenabwehr”, i *Computer und Recht*, 10/2015, sidorna 665–670.

54. Oavsett hur denna kontrovers i den nationella rätten beskrivs, bör domstolen då den svarar begränsa sig till att tolka de två bestämmelser i direktiv 95/46 som den nationella domstolen och parterna i målet har hänvisat till, det vill säga artikel 2 a [12] och skäl 26. [13]

55. Enbart genom att tillhandahålla information om datum och klockslag då en webbplats har använts från en viss dator (eller annan enhet), visar de dynamiska IP-adresserna vissa beteendemönster hos internetanvändarna och därmed innebär de ett potentiellt intrång i rätten till skydd för användarnas privatliv. [14] Denna rätt garanteras genom artikel 8 i Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna och genom artikel 7 i stadgan, mot bakgrund av vilken, jämte artikel 8 i densamma, direktiv 95/46 ska tolkas. [15] I själva verket har parterna i målet inte ifrågasatt denna förutsättning och den är heller inte i sig föremål för begäran om förhandsavgörande.

56. Den person som dessa uppgifter rör är inte en ”identifierad fysisk person”. En uppgift om vilket datum och klockslag som anslutningen skedde, eller från vilket nummer, visar varken direkt eller omedelbart vilken fysisk person som innehar den enhet från vilken webbplatsen användes och inte heller vilken användare som hanterar den (och som kan vara vilken fysisk person som helst).

57. Eftersom en dynamisk IP-adress hjälper till att avgöra – antingen i sig eller i kombination med andra uppgifter – vem som innehar den enhet som har använts för att ansluta sig till webbplatsen, kan den betecknas som information om en ”identifierbar person”. [16]

58. Enligt Bundesgerichtshofs resonemang är den dynamiska IP-adressen inte i sig tillräcklig för att identifiera den användare som med hjälp av denna adress har använt en webbplats. Om tjänsteleverantören däremot hade kunnat identifiera användaren med hjälp av den dynamiska IP-adressen, hade det utan tvekan rört sig om en personuppgift i den mening som avses i direktiv 95/46. Detta förefaller emellertid inte vara innebörden av tolkningsfrågan, vilken förutsätter att de tjänsteleverantörer som är inblandade i det nationella målet inte kan identifiera användaren enbart med hjälp av den dynamiska IP-adressen.

59. I kombination med andra uppgifter, möjliggör den dynamiska IP-adressen en ”indirekt” identifiering av användaren, vilket alla parter är eniga om. Innebär möjligheten att det finns sådana ytterligare uppgifter som kan förknippas med den dynamiska IP-adressen, att denna adress utan vidare kan betecknas som en personuppgift i den mening som avses i direktivet? Det måste prövas huruvida det för detta ändamål räcker att det enbart finns en abstrakt möjlighet att få kännedom om dessa uppgifter eller om det krävs att de är tillgängliga för den som redan känner till den dynamiska IP-adressen eller för en tredje man.

12 — Vilken återgetts i punkt 13.

13 — Vilket återgetts i punkt 11.

14 — Detta erinrade generaladvokaten Cruz Villalón om i sitt förslag till avgörande i målet Scarlet Extended (C-70/10, EU:C:2011:255), punkt 76, och det ansåg även Europeiska datatillsynsmannen i sina yttranden av den 22 februari 2010 över EU:s pågående förhandlingar om ett handelsavtal om åtgärder mot varumärkesförfalskning (Acta-avtalet) (EUT, 2010, C 147, s. 1, punkt 24), och av den 10 maj 2010 om förslaget till Europaparlamentets och rådets direktiv om bekämpande av sexuella övergrepp mot barn, sexuell exploatering av barn och barnpornografi samt om upphävande av rambeslut 2004/68/RIF (EUT 2010, C 323, s. 6, punkt 11).

15 — Se, för ett liknande resonemang, dom av den 20 maj 2003, Österreichischer Rundfunk (C-465/00, C-138/01 och C-139/01, EU:C:2003:294), punkt 68, samt generaladvokaten Kokotts förslag till avgörande i målet Promusicae (C-275/06, EU:C:2007:454), punkt 51 och följande punkter.

16 — Om inte motsatsen bevisas, kan det presumeras att det är den personen som har surfat på internet och besökt webbplatsen i fråga. Även om detta inte presumeras gör informationen om datum och klockslag och från vilket nummer webbplatsen besöktes, det möjligt att koppla denna användning till innehavaren av enheten och direkt sätta den i samband med hans eller hennes beteendemönster på internet. Möjliga undantag skulle kunna vara IP-adresser som tilldelas datorer i lokaler som internetkaféer, vars anonyma användare inte kan identifieras och beträffande vars ägare den trafik som sker i lokalen inte ger någon relevant personlig information. Detta är för övrigt det enda undantag från principen att IP-adresser utgör personuppgifter som godtagits av Arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter, vilken inrättades genom direktiv 95/46 (den så kallade artikel 29-gruppen). Se dess yttrande 4/2007 av den 20 juni 2007 om begreppet personuppgifter, WP 136,
påhttp://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

60. Parterna har i sina yttranden koncentrerat sig på tolkningen av skäl 26 i direktiv 95/46, i vilket de framhållit formuleringen ”hjälpmedel som i syfte att identifiera vederbörande rimligen kan komma att användas antingen av den registeransvarige eller av någon annan person”. Den hänskjutande domstolens fråga gäller inte ytterligare uppgifter som de berörda tjänsteleverantörerna i det nationella målet förfogar över. Den handlar heller inte om vilken tredje man som helst som förfogar över dessa ytterligare uppgifter (som i kombination med den dynamiska IP-adressen möjliggör en identifiering av användaren), utan om internetleverantören.

61. Det är således inte nödvändigt att domstolen granskar alla de hjälpmedel som motparten i det nationella målet ”rimligen” kan komma att använda sig av, för att de dynamiska IP-adresser som denne förfogar över ska kunna betecknas som personuppgifter. Eftersom Bundesgerichtshof bara har hänvisat till ytterligare uppgifter som en tredje man förfogar över, kan slutsatsen dras antingen a) att motparten inte har några egna ytterligare uppgifter som gör det möjligt att identifiera användaren, eller b) att motparten förfogar över sådana uppgifter men inte har någon rimlig möjlighet att använda dem för detta syfte, i egenskap av registeransvarig, enligt skäl 26 i direktiv 95/46.

62. Båda dessa alternativ är beroende av en prövning av de faktiska omständigheterna som det enbart ankommer på den hänskjutande domstolen att göra. EU-domstolen skulle ha kunnat tillhandahålla allmänna kriterier för att tolka uttrycket ”hjälpmedel som rimligen kan komma att användas av den registeransvarige”, om Bundesgerichtshof hade hyst tvivel om motpartens förmåga att rimligen använda sig av egna ytterligare uppgifter. Eftersom så inte är fallet är det enligt min uppfattning inte aktuellt att domstolen nu ska tillhandahålla tolkningskriterier som inte är nödvändiga för den hänskjutande domstolen och som den inte har efterfrågat.

63. Kärnan i den hänskjutna tolkningsfrågan är således huruvida det, för att dynamiska IP-adresser ska betecknas som personuppgifter, är av betydelse att en alldeles särskild tredje man – internetleverantören – förfogar över ytterligare uppgifter som i kombination med IP-adresserna gör det möjligt att identifiera den användare som har använt en viss webbplats.

64. Även här finns det anledning att hänvisa till skäl 26 i direktiv 95/46. Formuleringen ”hjälpmedel som ... rimligen kan komma att användas ... *av någon annan person*” [17] skulle kunna ge upphov till en tolkning som innebär att det skulle räcka att en tredje man skulle kunna skaffa fram ytterligare uppgifter (som kan kombineras med en dynamisk IP-adress för att identifiera en person), för att denna adress i sig skulle anses utgöra en personuppgift.

65. En sådan maximalistisk tolkning skulle i praktiken medföra att alla typer av information skulle anses vara personuppgifter, hur otillräcklig den än är i sig för att göra det möjligt att identifiera en användare. Det kan aldrig helt säkert uteslutas att det finns en tredje man som förfogar över ytterligare uppgifter som kan kombineras med den informationen och som därmed kan bidra till att röja en persons identitet.

66. Möjligheten att utvecklingen av de tekniska hjälpmedlen inom en inte alltför avlägsen framtid banar väg för allt mer sofistikerade instrument för att inhämta och behandla information, motiverar enligt min uppfattning de försiktighetsåtgärder med vilka man vill värna om integritetsskyddet. När man har definierat de rättsliga kategorier som är relevanta inom dataskyddsområdet, har man försökt att innefatta tillräckligt vida och flexibla fall med beteenden för att det ska täcka alla upptänkliga situationer. [18]

17 — Ingen kursivering i originalet.

18 — Denna vilja att förebygga ligger till grund för den ståndpunkt som Artikel 29-gruppen intagit. Den innebär att man ska utgå från principen att IP-adresserna utgör personuppgifter, och att det enda undantaget är de fall då tjänsteleverantören med full säkerhet kan avgöra att adresserna tillhör oidentifierbara personer, exempelvis användare på ett internetkafé. Se fotnot 16, in fine.

67. Jag anser emellertid att denna omsorg – vilken för övrigt är fullt legitim – inte får medföra att man bortser från lagstiftarens syfte och att den systematiska tolkningen av skäl 26 i direktiv 95/46 endast avser ”hjälpmedel som rimligen kan komma att användas” *av vissa andra personer*.

68. På samma sätt som skäl 26 inte avser vilka hjälpmedel som helst som kan användas av den registeransvarige (i det här fallet tjänsteleverantören), utan bara de som denne ”rimligen” kan komma att använda, måste det även uppfattas så, att lagstiftaren syftar på de ”andra personer” som en registeransvarig, som vill få fram de ytterligare uppgifterna för identifiering, *även här rimligen* kan komma att vända sig till. Så är inte fallet om kontakten med dessa andra personer i själva verket är mycket kostsam i personellt och ekonomiskt hänseende, eller ogenomförbar i praktiken eller förbjuden i lag. I annat fall skulle det, som jag tidigare nämnt, vara praktiskt taget omöjligt att göra skillnad mellan olika hjälpmedel, eftersom det alltid går att föreställa sig ett fall där en tredje man kan komma att ha tillgång till ytterligare uppgifter som är relevanta för att en användare ska kunna identifieras, hur oåtkomliga dessa än är för tjänsteleverantören – nu eller i framtiden.

69. Som jag tidigare har påpekat är den tredje man som Bundesgerichtshof syftar på en internetleverantör. Det är säkert till denna tredje man som det är rimligast att tänka sig att tjänsteleverantören vänder sig för att inhämta de ytterligare uppgifter som krävs, om denne har för avsikt att på det mest effektiva, praktiska och direkta sättet identifiera den användare som har använt hans webbplats med hjälp av den dynamiska IP-adressen. Det är inte på något sätt en hypotetisk, okänd eller oåtkomlig tredje man, utan en protagonist i det nätverk som internet utgör, och man vet med säkerhet att denne tredje man förfogar över de uppgifter som tjänsteleverantören behöver för att identifiera användaren. Det är enligt vad den hänskjutande domstolen uppger till just denna tredje man som motparten i det nationella målet har för avsikt att vända sig för att inhämta de ytterligare uppgifter som denne behöver.

70. En internetleverantör är ett typexempel på en sådan tredje man som avses i skäl 26 i direktiv 95/46, till vilken det är ”rimligast” att tjänsteleverantören i det nationella målet kan komma att vända sig. Det återstår emellertid att klarlägga huruvida inhämtandet av de ytterligare uppgifter som denne tredje man förfogar över kan anses vara ”rimligen” genomförbart.

71. Den tyska regeringen har gjort gällande att eftersom den information som internetleverantören förfogar över utgör en personuppgift, kan denne inte tillhandahålla den utan vidare, utan endast i enlighet med de bestämmelser som reglerar behandlingen av sådana uppgifter. [19]

72. Utan tvekan är det så, eftersom man måste följa den lagstiftning som är tillämplig på personuppgifter för att få tillgång till den informationen. Information kan ”rimligen” bara inhämtas om villkoren för att få tillgång till den typen av uppgifter är uppfyllda, av vilket det första är att det ska finnas stöd i lag för att lagra dem och överföra dem till andra. Internetleverantören har rätt att vägra att lämna ut de begärda uppgifterna, men även det motsatta är möjligt. Möjligheten att överföra uppgifter, vilken är fullt ”rimlig”, innebär i sig att den dynamiska IP-adressen i enlighet med skäl 26 i direktiv 95/46 utgör en personuppgift för tjänsteleverantören.

73. Det är en möjlighet som är *tillåten enligt lag* och som därför är ”rimlig”. De rimliga hjälpmedel som avses i direktiv 95/46 måste per definition vara lagliga. [20] Detta är självfallet utgångspunkten för den hänskjutande domstolen, vilket den tyska regeringen har erinrat om. [21] Det innebär att de rättsligt relevanta sätten att få tillgång till uppgifterna avsevärt minskar, eftersom det enbart kan vara de som har stöd i lag. Så länge sådana finns, oavsett hur restriktiva de är i sin praktiska tillämpning, utgör de emellertid ett ”rimligt hjälpmedel” i den mening som avses i direktiv 95/46.

19 — Punkterna 40 och 45 i dess skriftliga yttrande.

20 — Det är i detta sammanhang irrelevant om det är möjligt att de facto få tillgång till personuppgiften genom att bryta mot dataskyddslagstiftningen.

21 — Punkterna 47 och 48 i dess skriftliga yttrande.

74. Följaktligen anser jag att den första tolkningsfrågan, så som den har formulerats av Bundesgerichtshof, ska besvaras jakande. Den dynamiska IP-adressen ska anses vara en personuppgift för tjänsteleverantören, eftersom det finns en tredje man (internetleverantören) som denne rimligen kan vända sig till för att få fram ytterligare uppgifter, vilka i kombination med IP-adressen gör att användaren kan identifieras.

75. Det resultat som skulle bli följden av en motsatt lösning till den jag föreslår anser jag talar för mitt förslag. Om de dynamiska IP-adresserna inte skulle utgöra personuppgifter för tjänsteleverantören, skulle denne kunna lagra dem på obestämd tid och när som helst vända sig till internetleverantören och begära att få tillgång till de ytterligare uppgifterna för att kombinera dem med IP-adressen och identifiera användaren. Såsom den tyska regeringen har medgett,[22] blir den dynamiska IP-adressen under dessa förhållanden en personuppgift, eftersom tjänsteleverantören då redan har de ytterligare uppgifter som krävs för att identifiera användaren, vilket innebär att dataskyddlagstiftningen ska tillämpas.

76. Det rör sig om en uppgift som det bara varit möjligt att lagra på grund av att den dittills inte ansetts vara en personuppgift för tjänsteleverantören. Det är således upp till tjänsteleverantören om den dynamiska IP-adressen i rättsligt hänseende ska betecknas som en personuppgift. Detta är beroende av om han vid en framtida tidpunkt bestämmer sig för att använda den för att identifiera användaren genom att kombinera den med de ytterligare uppgifter som han måste inhämta från en tredje man. Min uppfattning är emellertid att enligt direktiv 95/46 är det avgörande att det finns en – rimlig – möjlighet att det existerar en tredje man som är ”tillgänglig” och som förfogar över de hjälpmedel som krävs för att kunna identifiera en person, och inte att möjligheten att vända sig till denna tredje man verkligen utnyttjas.

77. Det kan till och med medges, vilket den tyska regeringen har gjort, att den dynamiska IP-adressen blir en personuppgift först då internetleverantören tar emot den. Det bör då godtas att denna kvalificering har skett med retroaktiv verkan, vad beträffar lagringstiden för IP-adressen, och därmed bör IP-adressen betraktas som icke-existerande, om den tid har löpt ut under vilken den hade fått lagras om den redan från början hade kvalificerats som en personuppgift. I det fallet skulle ett resultat erhållas som strider mot andemeningen i dataskyddslagstiftningen. Skälet till att dessa uppgifter endast får lagras under en begränsad tid skulle undergrävas om betydelsen av en egenskap som finns hos dem redan från början – deras verkan som hjälpmedel för att identifiera en fysisk person, i sig eller i kombination med andra uppgifter – eventuellt skulle skjutas upp. Även av detta skäl, som är rent ekonomiskt, är det rimligare att tillskriva den denna egenskap redan från början.

78. Således anser jag, som slutsats i denna del, att artikel 2 a i direktiv 95/46/EG ska tolkas så, att en IP-adress som en tjänsteleverantör lagrar i samband med att någon använder tjänsteleverantörens webbplats utgör en personuppgift för denne, i den mån en internetleverantör förfogar över de ytterligare uppgifter som krävs för att identifiera den registrerade.

B – *Den andra frågan*

79. I sin andra tolkningsfråga undrar Bundesgerichtshof om artikel 7 f i direktiv 95/46 utgör hinder för en bestämmelse i nationell rätt enligt vilken en tjänsteleverantör endast kan samla in och använda personuppgifter för en användare utan dennes samtycke i den mån detta krävs för att möjliggöra, och ta betalt för, den aktuella användarens konkreta användning av teletjänsten och enligt vilken syftet att säkerställa tjänstens allmänna funktion inte kan rättfärdiga en användning efter det att den aktuella sessionen har avslutats.

22 — Punkt 36 i dess skriftliga yttrande.

80. Innan jag svarar bör ett påpekande göras beträffande den information som Bundesgerichtshof har tillhandahållit. Enligt denna lagras de aktuella uppgifterna för att säkerställa de aktuella webbplatsernas allmänna funktion och för att i förekommande fall möjliggöra lagföring av it-angrepp som de utsätts för.

81. Det måste således till att börja med klarläggas huruvida behandlingen av de IP-adresser som nämns i beslutet att begära förhandsavgörande, omfattas av det undantag som föreskrivs i artikel 3.2 första strecksatsen i direktiv 95/46. [23]

1. Huruvida direktiv 95/46 är tillämpligt på behandlingen av de aktuella uppgifterna

82. Förbundsrepubliken Tyskland förefaller i det nationella målet enbart handla som en tjänsteleverantör, det vill säga som en enskild (och således utan befogenheter). Av denna omständighet kan slutsatsen dras att behandlingen av de uppgifter som är aktuella i det här målet i princip inte är undantagen från tillämpningsområdet för direktiv 95/46.

83. Enligt vad domstolen slog fast i domen i målet Lindqvist, [24] avser den verksamhet som nämns i artikel 3.2 i direktiv 95/46 ”i samtliga fall sådan verksamhet som endast kan bedrivas av staten eller statliga myndigheter och som inte kan bedrivas av enskilda personer”. [25] Om den registeransvarige för de omtvistade uppgifterna trots sin ställning som offentlig myndighet i själva verket handlar som ett privaträttsligt subjekt, är direktiv 95/46 tillämpligt.

84. Den hänskjutande domstolen har betonat att de tyska myndigheternas huvudsyfte med att lagra de dynamiska IP-adresserna är att ”säkerställa och upprätthålla funktionsdugligheten för svarandens teletjänster”, i synnerhet för att ”upptäcka och avvärja de ofta förekommande ’Denial-of-Service’ -attackerna’. Vid dessa attacker lamslås en telekommunikationsinfrastruktur via riktad och koordinerad överbelastning av enstaka webbservrar genom en stor mängd anrop”. [26] Det är vanligt att innehavare av viktigare webbplatser lagrar dynamiska IP-adresser i detta syfte och det innebär inte någon myndighetsutövning, varken direkt eller indirekt. Det är därför inte särskilt svårt att hävda att de omfattas av tillämpningsområdet för direktiv 95/46.

85. Bundesgerichtshof har emellertid gjort gällande att de aktuella tjänsteleverantörernas lagring av de dynamiska IP-adresserna även syftar till att kunna vidta straffrättsliga åtgärder, om det blir aktuellt, mot dem som ligger bakom eventuella it-angrepp. Räcker detta syfte för att behandlingen av dessa uppgifter ska vara undantagen från tillämpningsområdet för direktiv 95/46?

86. Om man med ”straffrättsliga åtgärder” menar att de tjänsteleverantörer som är motparter i det nationella målet utövar statens befogenheter att utdöma straff, anser jag att det rör sig om ”statens verksamhet på straffrättens område” och således föreligger ett av de undantag som föreskrivs i artikel 3.2 första strecksatsen i direktiv 95/46.

87. Enligt vad domstolen slog fast i domen i målet Huber, [27] omfattas tjänsteleverantörernas behandling av personuppgifter för att upprätthålla säkerheten och funktionsdugligheten för sina teletjänster av tillämpningsområdet för direktiv 95/46, medan behandling av uppgifter för statens verksamhet på straffrättens område inte gör det.

23 — I tillämpningsområdet för direktiv 95/46 ingår inte ”behandlingar som rör allmän säkerhet, försvar, statens säkerhet … och *statens verksamhet på straffrättens område*” (ingen kursivering i originalet).

24 — Dom av den 6 november 2003 (C-101/01, EU:C:2003:596), punkt 43.

25 — För ett liknande resonemang, se dom av den 16 december 2008, Satakunnan Markkinapörssi och Satamedia (C-73/07, EU:C:2008:727), punkt 41.

26 — Punkt 36 i beslutet att begära förhandsavgörande.

27 — Dom av den 16 december 2008 (C-524/06, EU:C:2008:724), punkt 45.

88. Även om de straffrättsliga åtgärderna i egentlig mening inte vidtas av Förbundsrepubliken Tyskland, som bara är en tjänsteleverantör utan befogenheter, utan att denna, som vilken enskild som helst, endast överför de aktuella IP-adresserna till ett statligt organ för lagföring, syftar även här behandlingen av de dynamiska IP-adresserna till en verksamhet som är undantagen från tillämpningsområdet för direktiv 95/46.

89. Detta följer av domen i målet parlamentet/rådet och kommissionen,[28] i vilken domstolen slog fast att den omständigheten att vissa personuppgifter ”har samlats in av privata operatörer för kommersiella syften och att det är dessa operatörer som sköter överföringen av uppgifterna till en tredje stat” inte innebär att denna överföring ”faller utanför ... tillämpningsområde[t]” för artikel 3.2 första strecksatsen i direktiv 95/46 när syftet med överföringen rör statens verksamhet på straffrättens område, eftersom den då ”sker ... inom en ram som inrättats av statsmakterna och som avser allmän säkerhet”.[29]

90. Om däremot ”straffrättsliga åtgärder”, som jag anser och vilket följer av beslutet att begära förhandsavgörande, avser åtgärder som en enskild vidtar i egenskap av behörig att yrka att staten ska utöva sina befogenheter att utdöma straff, genom att väcka talan om detta, kan det inte göras gällande att behandlingen av de dynamiska IP-adresserna syftar till statens verksamhet på straffrättens område, vilken är undantagen från tillämpningsområdet för direktiv 95/46.

91. Lagringen och registreringen av denna uppgift kan tjäna som ytterligare ett bevismedel med hjälp av vilket innehavaren av webbplatsen kan begära att staten, på yrkande av part, ska lagföra ett rättsstridigt handlande. Den utgör således ett instrument för att på straffrättslig väg försvara de rättigheter som rättsordningen tillerkänner ett enskilt subjekt (i det här fallet ett offentligt organ som handlar enligt privaträttsliga regler). Den skiljer sig i det avseendet inte från ett initiativ från vilken annan tjänsteleverantör som helst som vill ha statens skydd i enlighet med de förfaranden för straffrättslig talan som föreskrivs i rättsordningen.

92. I den mån de tyska myndigheterna handlar som tjänsteleverantörer utan myndighetsbefogenheter, vilket det ankommer på den hänskjutande domstolen att pröva, omfattas deras behandling av dynamiska IP-adresser, genom att de utgör personuppgifter, av tillämpningsområdet för direktiv 95/46.

2. Prövning i sak

93. 15 § punkt 1 TMG tillåter bara att en användares personuppgifter samlas in och används i den mån detta krävs för att möjliggöra, och ta betalt för, den aktuella användarens konkreta användning av teletjänsten. Närmare bestämt får tjänsteleverantören bara samla in och använda så kallade användningsdata, det vill säga personuppgifter rörande en användare som är nödvändiga för att möjliggöra ”användningen av teletjänsten samt faktureringen för detta”. Dessa uppgifter ska utplånas när sessionen är slut (det vill säga när användningen av den konkreta teletjänsten upphör), om de inte behöver sparas ”för faktureringen”, enligt vad som föreskrivs i 15 § punkt 4 TMG.

28 — Dom av den 30 maj 2006 (C-317/04 och C-318/04, EU:C:2006:346), punkterna 54–59.

29 — Ibidem, punkt 59. Målet handlade om personuppgifter vars behandling inte var nödvändig för att tillhandahålla de tjänster som utgjorde de berörda privata aktörernas affärsverksamhet (flygbolag), men som dessa såg sig tvingade att överföra till myndigheterna i USA för att förebygga och bekämpa terrorism.

94. Efter det att anslutningen upphört förefaller 15 § TMG utesluta att dessa användningsdata lagras för andra ändamål. De får således inte heller lagras för att generellt möjliggöra ”användningen av teletjänsten”. Genom att det bara anges att uppgifterna får lagras för faktureringen, skulle den bestämmelsen i TMG kunna tolkas (även om det ankommer på den hänskjutande domstolen att göra den slutgiltiga tolkningen) som om den föreskrev att användardata bara får användas för att möjliggöra en konkret förbindelse och att de ska utplånas när förbindelsen avslutas.

95. I artikel 7 f i direktiv 95/46 [30] tillåts behandling av personuppgifter på villkor som jag skulle vilja beteckna som mer generösa (för den registeransvarige) än dem som föreskrivs i 15 § TMG. Den tyska bestämmelsen skulle på denna punkt kunna anses vara mer restriktiv än den unionsrättsliga, eftersom den i princip inte möjliggör att något annat berättigat intresse tillgodoses än det som är knutet till faktureringen för tjänsten, samtidigt som Förbundsrepubliken Tyskland i egenskap av tjänsteleverantör även skulle kunna ha ett berättigat intresse av att säkerställa sina webbplatsers allmänna funktion, utöver varje användningsförbindelse. [31]

96. Domstolens dom i målet ASNEF och FECEMD [32] innehåller riktlinjer för att besvara den andra tolkningsfrågan. Domstolen slog där fast att det av ändamålet med direktiv 95/46 ”framgår ... att det i artikel 7 i direktiv 95/46 görs en uttömmande uppräkning av de situationer när en behandling av personuppgifter kan anses vara tillåten”. [33] Härav följer att ”medlemsstaterna varken får foga ytterligare principer för tillåtligheten av behandlingen av personuppgifter till dem som nämns i artikel 7 i direktiv 95/46 eller föreskriva ytterligare villkor som påverkar räckvidden av de sex principer som föreskrivs i nämnda artikel”. [34]

97. 15 § TMG fogar inte något ytterligare villkor till dem som föreskrivs i artikel 7 i direktiv 95/46 för att behandlingen av uppgifter ska vara tillåten – vilket var fallet i målen ASNEF och FECEMD [35] – men om den tolkas på det restriktiva sätt som den hänskjutande domstolen har hänvisat till, minskar den innehållet i det villkor som föreskrivs i punkt f i denna artikel. Medan unionslagstiftaren generellt hänvisar till ”… ändamål som rör berättigade intressen hos den registeransvarige eller hos den eller de tredje män till vilka uppgifterna har lämnats ut”, beaktas i 15 § TMG endast behovet av att ”möjliggöra användningen av [den konkreta] teletjänsten samt faktureringen för detta”.

98. Såsom var fallet i målen ASNEF och FECEMD, [36] skulle även i förevarande mål en nationell åtgärd – om den tolkas på det restriktiva sätt som tidigare nämnts – ändra räckvidden av en princip i artikel 7 i direktiv 95/46, snarare än att bara precisera den, vilket är det enda myndigheterna i varje medlemsstat får göra med ett visst utrymme för skönsmässig bedömning, i enlighet med artikel 5 i direktiv 95/46.

30 — Vilken återgetts i punkt 17.

31 — Se punkt 84. Webbplatsinnehavarna har visserligen ett berättigat intresse av att förebygga och bekämpa de ”Denials of Service”-attacker som den hänskjutande domstolen har hänvisat till, det vill säga sådana massiva angrepp som ibland på ett koordinerat sätt riktas mot vissa webbplatser för att överbelasta och lamslå dem.

32 — Dom av den 24 november 2011 (C-468/10 och C-469/10, EU:C:2011:777).

33 — Ibidem, punkt 30.

34 — Ibidem, punkt 32.

35 — Ett fall där det i den nationella lagstiftningen, utöver kraven i artikel 7 f i direktiv 95/46, tillades att de uppgifter som var föremål för behandling skulle finnas i allmänt tillgängliga källor.

36 — Dom av den 24 november 2011 (C-468/10 och C-469/10, EU:C:2011:777).

99. Enligt den sistnämnda bestämmelsen ska ”[m]edlemsstaterna ... inom de begränsningar som bestämmelserna i detta kapitel innebär,[37] precisera på vilka villkor behandling av personuppgifter är tillåten”. Såsom domstolen slog fast i domen i målen ASNEF och FECEMD,[38] får medlemsstaterna emellertid ”enligt artikel 5 i direktiv 95/46, inte heller ... föreskriva ytterligare principer för tillåtligheten av behandlingen av personuppgifter än dem som räknas upp i artikel 7 i direktivet eller föreskriva ytterligare villkor som påverkar räckvidden av de sex principer som föreskrivs i nämnda artikel”.

100. I jämförelse med artikel 7 f i direktiv 95/46 minskar 15 § TMG avsevärt omfattningen av det berättigade intresse som är relevant för att motivera behandling av uppgifter och den begränsar sig inte till att enbart precisera eller nyansera det inom ramen för vad som är tillåtet enligt artikel 5 i direktivet. Den gör det dessutom på ett otvetydigt och absolut sätt, utan att medge att en avvägning kan göras mellan skyddet och säkerställandet av den allmänna användningen av teletjänsten och ”den registrerades intressen eller dennes grundläggande fri- och rättigheter som kräver skydd under artikel 1.1” i direktiv 95/46, enligt vad som föreskrivs i artikel 7 f i direktivet.

101. Liksom i målen ASNEF och FECEMD,[39] har den tyska lagstiftaren angett ”för [vissa typer av personuppgifter] ... 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” vilket innebär att det ”inte längre [rör sig] om en precisering i den mening som avses i ... artikel 5” i direktiv 95/46.

102. Mot bakgrund av detta anser jag att Bundesgerichtshof är skyldig att tolka den nationella lagstiftningen på ett sätt som överensstämmer med direktiv 95/46, vilket innebär a) att man till de skäl som motiverar behandling av så kallade användningsdata får foga teletjänstleverantörens berättigade intresse av att generellt skydda användningen av dessa tjänster och b) att en avvägning får göras i det enskilda fallet mellan tjänsteleverantörens intresse och användarens intresse eller grundläggande rättigheter och friheter, för att klarlägga vilket intresse som ska åtnjuta skydd enligt artikel 1.1 i direktiv 95/46.[40]

103. Det finns enligt min uppfattning inget ytterligare att tillägga beträffande villkoren för hur denna avvägning ska göras i det fall som har föranlett förevarande begäran om förhandsavgörande. Bundesgerichtshof har inte ställt någon fråga beträffande detta, utan den har inriktat sig på en fråga som föregår denna avvägning, nämligen huruvida en sådan avvägning kan göras.

104. Det behöver avslutningsvis knappast påpekas att den nationella domstolen får beakta eventuella lagbestämmelser som medlemsstaten har antagit inom ramen för vad som är tillåtet enligt artikel 13.1 d i direktiv 95/46, för att begränsa omfattningen av de rättigheter och skyldigheter som föreskrivs i artikel 6 i direktivet, i fall då en sådan begränsning är en nödvändig åtgärd med hänsyn till bland annat ”… förebyggande, undersökning, avslöjande av brott eller åtal för brott …”. Inte heller detta har den hänskjutande domstolen hänvisat till, trots att den utan tvekan känner till dessa båda artiklar.

105. Följaktligen föreslår jag att den andra tolkningsfrågan ska besvaras så, att artikel 7 f i direktiv 95/46 utgör hinder för en nationell bestämmelse enligt vilken en tjänsteleverantör inte får samla in och behandla personuppgifter för en användare, utan dennes samtycke, i syfte att säkerställa teletjänstens allmänna funktion, efter det att den aktuella sessionen har avslutats.

37 — Kapitel II, som har rubriken ”Allmänna bestämmelser om när personuppgifter får behandlas” och som innehåller artiklarna 5–21 i direktiv 95/46.

38 — Dom av den 24 november 2011 (C-468/10 och C-469/10, EU:C:2011:777), punkt 36.

39 — Ibidem, punkt 47.

40 — Vid förhandlingen gjorde Breyers ombud gällande att lagringen av de dynamiska IP-adresserna inte är nödvändig för att säkerställa att internettjänsterna fungerar väl mot eventuella angrepp. Jag anser inte att man kan tillhandahålla någon absolut lösning på detta problem. I varje enskilt fall måste det först göras en avvägning mellan webbplatsinnehavarens intresse och användarnas rättigheter och intressen.

VI – Förslag till avgörande

106. Med hänsyn till vad som anförts ovan föreslår jag att domstolen besvarar de tolkningsfrågor som ställts enligt följande:

”1) Enligt 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, utgör en dynamisk IP-adress med hjälp av vilken en användare har använt en webbplats tillhörande en leverantör av teletjänster, en ”personuppgift” för denne när en internetleverantör förfogar över de ytterligare uppgifter som tillsammans med den dynamiska IP-adressen gör det möjligt att identifiera användaren.

2) Artikel 7 f i direktiv 95/46 ska tolkas så, att syftet att säkerställa teletjänstens allmänna funktion i princip ska anses vara ett berättigat intresse som rättfärdigar behandlingen av denna personuppgift, förutsatt att det anses ha företräde framför den registrerades intresse eller grundläggande rättigheter. En nationell bestämmelse som inte gör det möjligt att beakta detta berättigade intresse är oförenlig med nämnda artikel.”