Samling af Afgørelser

FORSLAG TIL AFGØRELSE FRA GENERALADVOKAT
M. CAMPOS SÁNCHEZ-BORDONA
fremsat den 12. maj 2016 [1]

Sag C-582/14

Patrick Breyer
mod
Bundesrepublik Deutschland

(anmodning om præjudiciel afgørelse indgivet af Bundesgerichtshof (forbundsdomstol, Tyskland))

»Behandling af personoplysninger — direktiv 95/46/EF — artikel 2, litra a), og artikel 7, litra f) — begrebet »personoplysninger« — ip-adresser — opbevaring hos en udbyder af elektroniske medietjenester — national lovgivning, der ikke giver mulighed for at tage højde for den legitime interesse, som den registeransvarlige forfølger«

1. En internetprotokol-adresse (herefter »ip-adresse«) er en rækkefølge af cifre, der tildeles en anordning (en computer, en tablet, en smartphone), og som identificerer den og giver den mulighed for at få adgang til det elektroniske telekommunikationsnet. For at få adgang til internettet skal anordningen anvende den rækkefølge af cifre, som den er blevet tildelt af udbyderne af netadgangstjenesten. Ip-adressen meddeles til den server, som det besøgte websted er lagret på.

2. Internetudbydere (som oftest teleselskaber) tildeler sine kunder såkaldte »dynamiske ip-adresser« midlertidigt for hver enkelt internettilslutning og ændrer dem næste gang, der oprettes forbindelse. Disse virksomheder fører et register over samtlige ip-adresser, der er tildelt en bestemt anordning [2].

3. Indehaverne af de websteder, som brugerne får adgang til ved hjælp af de dynamiske ip-adresser, fører som regel også registre over, hvilke websteder der er blevet besøgt, hvornår samt fra hvilken dynamisk ip-adresse. Det er teknisk set muligt at lagre denne registrering uden tidsmæssige begrænsninger, når den enkelte brugers internetforbindelse er afsluttet.

4. En dynamisk ip-adresse er ikke i sig selv tilstrækkelig til, at tjenesteudbyderen kan identificere brugeren af dennes websted. Dette kan den imidlertid, hvis den kombinerer den dynamiske ip-adresse med andre oplysninger, som internetudbyderen råder over.

1 — Originalsprog: spansk.

2 — Artikel 5 i Europa-Parlamentets og Rådets direktiv 2006/24/EF af 15.3.2006 om lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet og om ændring af direktiv 2002/58/EF (EUT 2006, L 105, s. 54) fastlagde flere forpligtelser, heriblandt at lagre »dato og klokkeslæt for ind- og udlogning af internetadgangstjenester [...] og den dynamiske eller statiske ip-adresse, som udbyderen af internetadgangstjenesten har tildelt en kommunikation, samt brugeridentitet på abonnenten eller den registrerede bruger« med henblik på efterforskning, afsløring og retsforfølgning af alvorlige overtrædelser.

5. I denne sag er det omtvistet, hvorvidt dynamiske ip-adresser er en personoplysning som omhandlet i artikel 2, litra a), i direktiv 95/46/EF [3]. Spørgsmålet kræver først og fremmest en afgørelse af, hvilken betydning det har, at det ikke er indehaveren af webstedet, men derimod tredjemand (internetudbyderen i denne sag), der råder over de yderligere oplysninger, som er nødvendige for at identificere brugeren.

6. Det er et nyt spørgsmål for Domstolen, som i præmis 51 i dommen i sagen Scarlet Extended [4] konstaterede, at ip-adresser er »beskyttede personoplysninger, fordi de gør det muligt præcist at identificere de nævnte brugere«. Dette skete imidlertid i en sag, hvor internetudbyderen [5], og ikke en udbyder af indhold, foretog indsamlingen og identificeringen af ip-adresserne, således som det er tilfældet i nærværende sag.

7. Såfremt de dynamiske ip-adresser er personoplysninger for udbyderen af internettjenester, skal det derefter undersøges, om behandlingen heraf er omfattet af anvendelsesområdet af direktiv 95/46.

8. Det er muligt, at de, selv om de er personoplysninger, ikke er omfattet af beskyttelsen i henhold til direktiv 95/46, hvis målet med behandlingen af dem eksempelvis er at træffe strafferetlige foranstaltninger mod eventuelle angreb på webstedet. I dette tilfælde finder direktiv 95/46 ikke anvendelse i henhold til artikel 3, stk. 2, første led.

9. Det skal ligeledes afgøres, om den internetudbyder, der registrerer de dynamiske ip-adresser, når en bruger får adgang til dennes websteder (Forbundsrepublikken Tyskland i denne sag) agerer som en offentlig myndighed eller nærmere som en privatperson.

10. Såfremt direktiv 95/46 finder anvendelse, skal det endelig præciseres, i hvilket omfang dette direktivs artikel 7, litra f), er forenelig med en national lovgivning, som begrænser omfanget af en af de i artiklen fastlagte betinger for at begrunde behandlingen af personoplysninger.

I – Retsforskrifter

A – *EU-retten*

11. 26. betragtning til direktiv 95/46 har følgende ordlyd:

»(26) Beskyttelsesprincipperne skal gælde enhver oplysning om en identificeret eller identificerbar person; for at afgøre, om en person er identificerbar, tages alle de hjælpemidler i betragtning, der med rimelighed kan tænkes bragt i anvendelse for at identificere den pågældende enten af den registeransvarlige eller af enhver anden person; beskyttelsesprincipperne gælder ikke oplysninger, som er gjort anonyme på en sådan måde, at den registrerede ikke længere kan identificeres; adfærdskodekser i henhold til artikel 27 kan være et nyttigt instrument til at angive måder, hvorpå oplysningerne kan gøres anonyme og opbevares i en sådan form, at den registrerede ikke længere kan identificeres.«

3 — Europa-Parlamentet og Rådets direktiv af 24.10.1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (EFT 1995, L 281, s. 31).

4 — Dom af 24.11.2011 (C-70/10, EU:C:2011:771, præmis 51).

5 — Det samme var tilfældet i dom af 19.4.2012, Bonnier Audio m.fl. (C-461/10, EU:C:2012:219, præmis 51 og 52).

12. Artikel 1 i direktiv 95/46 har følgende ordlyd:

»1. Medlemsstaterne sikrer i overensstemmelse med dette direktiv beskyttelsen af fysiske personers grundlæggende rettigheder og frihedsrettigheder, især retten til privatlivets fred, i forbindelse med behandling af personoplysninger.

2. Medlemsstaterne må ikke af grunde, der har forbindelse med den i stk. 1 foreskrevne beskyttelse, indskrænke eller forbyde fri udveksling af personoplysninger mellem medlemsstaterne.«

13. Artikel 2 i direktiv 95/46 bestemmer:

»I dette direktiv forstås ved:

a) »personoplysninger« enhver form for information om en identificeret eller identificerbar fysisk person (»den registrerede«); ved identificerbar person forstås en person, der direkte eller indirekte kan identificeres, bl.a. ved et identifikationsnummer eller et eller flere elementer, der er særlige for denne persons fysiske, fysiologiske, psykiske, økonomiske, kulturelle eller sociale identitet

b) »behandling af personoplysninger« (»behandling«) enhver operation eller række af operationer – med eller uden brug af elektronisk databehandling – som personoplysninger gøres til genstand for, f.eks. indsamling, registrering, systematisering, opbevaring, tilpasning eller ændring, selektion, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring samt blokering, slettelse eller tilintetgørelse

[…]

d) »den registeransvarlige« den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der alene eller sammen med andre afgør, til hvilket formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger; er formålet med og hjælpemidlerne ved behandlingen fastlagt ved nationale love eller forskrifter eller på fællesskabsplan, kan den registeransvarlige, eller de specifikke kriterier for udpegelse af denne, angives i den pågældende nationale ret eller i fællesskabsretten

[…]

f) »tredjemand« enhver anden fysisk eller juridisk person, offentlig myndighed, institution eller ethvert andet organ end den registrerede, den registeransvarlige, registerføreren og de personer under den registeransvarliges eller registerførerens direkte myndighed, der er beføjet til at behandle oplysningerne

[…]«

14. Under overskriften »Anvendelsesområde« bestemmer artikel 3 i direktiv 95/46:

»1. Dette direktivs bestemmelser anvendes på behandling af personoplysninger, der helt eller delvis foretages ved hjælp af edb, samt på ikke-elektronisk behandling af personoplysninger, der er eller vil blive indeholdt i et register.

2. Dette direktiv gælder ikke for sådan behandling af personoplysninger,

— som iværksættes med henblik på udøvelse af aktiviteter, der ikke er omfattet af fællesskabsretten, som f.eks. de aktiviteter, der er fastsat i afsnit V og VI i traktaten om Den Europæiske Union, og under ingen omstændigheder for behandling, der vedrører den offentlige sikkerhed, forsvar, statens sikkerhed (herunder statens økonomiske interesser, når behandlingen er forbundet med spørgsmål vedrørende statens sikkerhed) og statens aktiviteter på det strafferetlige område

[…]«

15. Kapitel II i direktiv 95/46 om »Almindelige betingelser for lovlig behandling af personoplysninger« indledes med artikel 5, som bestemmer, at »[m]edlemsstaterne præciserer i henhold til bestemmelserne i dette kapitel, på hvilke betingelser behandling af personoplysninger er lovlig«.

16. Artikel 6 i direktiv 95/46 har følgende ordlyd:

»1. Medlemsstaterne fastsætter bestemmelser om, at personoplysninger

a) skal behandles rimeligt og lovligt

b) skal indsamles til udtrykkeligt angivne og legitime formål, samt at senere behandling heraf ikke må være uforenelig med disse formål; senere behandling af oplysninger i historisk, statistisk eller videnskabeligt øjemed anses ikke for at være uforenelig med disse formål, såfremt medlemsstaterne giver de fornødne garantier

c) skal være relevante og tilstrækkelige og ikke omfatte mere end, hvad der kræves til opfyldelse af de formål, hvortil de indsamles, og til de formål, hvortil de senere behandles

d) skal være korrekte og om nødvendigt ajourførte; der skal tages ethvert rimeligt skridt til at slette eller berigtige oplysninger, der er urigtige eller ufuldstændige i forhold til det formål, hvortil de indsamles, eller i forbindelse med hvilke de behandles på et senere tidspunkt

e) ikke må opbevares på en måde, der giver mulighed for at identificere de registrerede i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil de indsamles, eller i forbindelse med hvilke de behandles på et senere tidspunkt. Medlemsstaterne fastsætter de fornødne garantier for personoplysninger, der i historisk, statistisk eller videnskabeligt øjemed opbevares længere end i ovennævnte periode.

2. Det påhviler den registeransvarlige at sikre, at bestemmelserne i stk. 1 overholdes.«

17. Artikel 7 i direktiv 95/46 foreskriver:

»Medlemsstaterne fastsætter bestemmelser om, at behandling af personoplysninger kun må finde sted hvis:

a) der ikke hersker tvivl om, at den registrerede har givet sit samtykke, eller

b) behandlingen er nødvendig af hensyn til opfyldelsen af en kontrakt, som den registrerede er part i, eller af hensyn til gennemførelse af foranstaltninger, der træffes på dennes anmodning forud for indgåelsen af en sådan kontrakt, eller

c) behandlingen er nødvendig for at overholde en retlig forpligtelse, som gælder for den registeransvarlige, eller

d) behandlingen er nødvendig for at beskytte den registreredes vitale interesser, eller

e) behandlingen er nødvendig af hensyn til udførelsen af en opgave i samfundets interesse eller henhørende under offentlig myndighedsudøvelse, som den registeransvarlige eller en tredjemand, til hvem oplysningerne videregives, har fået pålagt, eller

f) behandlingen er nødvendig, for at den registeransvarlige eller den tredjemand eller de tredjemænd, til hvem oplysningerne videregives, kan forfølge en legitim interesse, medmindre den registreredes interesser eller de grundlæggende rettigheder og frihedsrettigheder, der skal beskyttes i henhold til artikel 1, stk. 1, i dette direktiv, går forud herfor.«

18. Artikel 13 i direktiv 95/46 bestemmer:

»1. Medlemsstaterne kan træffe lovmæssige foranstaltninger med henblik på at begrænse rækkevidden af de forpligtelser og rettigheder, der er omhandlet i artikel 6, stk. 1, artikel 10, artikel 11, stk. 1, samt artikel 12 og 21, hvis en sådan begrænsning er en nødvendig foranstaltning af hensyn til:

a) statens sikkerhed

b) forsvaret

c) den offentlige sikkerhed

d) forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager eller i forbindelse med brud på etiske regler for lovregulerede erhverv

e) væsentlige økonomiske eller finansielle interesser hos en medlemsstat eller Den Europæiske Union, herunder valuta-, budget- og skatteanliggender

f) en kontrol-, tilsyns- eller reguleringsopgave, selv af midlertidig karakter, der er et led i den offentlige myndighedsudøvelse på de i litra c), d) og e) nævnte områder

g) beskyttelsen af den registreredes interesser eller andres rettigheder og frihedsrettigheder.

[...]«

B – *National ret*

19. § 12 i Telemediengesetz (lov om telekommunikationstjenester, herefter »TMG«)[6] bestemmer:

»1. Tjenesteudbyderen må kun indsamle og anvende personoplysninger med henblik på at give adgang til telekommunikationstjenester, i det omfang dette er tilladt i henhold til denne lov eller en anden retsforskrift, der udtrykkelig vedrører telekommunikationstjenester, eller brugeren har givet sit samtykke hertil.

2. Tjenesteudbyderen må kun anvende personoplysninger, der er indsamlet med henblik på at give adgang til telekommunikationstjenester, til andre formål, i det omfang dette er tilladt i henhold til denne lov eller en anden retsforskrift, der udtrykkelig vedrører telekommunikationstjenester, eller brugeren har givet sit samtykke hertil.

3. Medmindre andet er bestemt, skal de gældende bestemmelser om beskyttelse af personoplysninger anvendes, også hvis oplysningerne ikke bearbejdes elektronisk.«

6 — Lov af 26.2.2007 (BGBl 2007 I, s. 179).

20. TMG's § 15 har følgende ordlyd:

»1. Tjenesteudbyderen må kun indsamle og anvende personoplysninger om en bruger, for så vidt som dette er nødvendigt for at give adgang til telekommunikationstjenester og afregne herfor (data om brugen). Data om brugen er navnlig

1. specifikationer til identificering af brugeren

2. oplysninger om påbegyndelse og afslutning af den pågældende brug og omfanget af brugen og

3. oplysninger om de telekommunikationstjenester, som brugeren har anvendt.

2. Tjenesteudbyderen er berettiget til at sammenføre data om en brugers anvendelse af forskellige telekommunikationstjenester, for så vidt det er nødvendigt af hensyn til afregningen over for vedkommende.

[…]

4. Tjenesteudbyderen er berettiget til at anvende data om brugen, også efter at den konkrete brug er afsluttet, for så vidt disse data er nødvendige af hensyn til afregningen over for brugeren (afregningsoplysninger). Tjenesteudbyderen er berettiget til at spærre oplysningerne med henblik på at opfylde opbevaringsfrister i henhold til gældende lov, vedtægt eller kontrakt. [...]«

21. § 3, stk. 1, i Bundesdatenschutzgesetz (forbundsloven om databeskyttelse, herefter »BDSG«)[7] bestemmer, at »personoplysninger er detaljer om personlige eller materielle forhold hos en identificeret eller identificerbar fysisk person (den berørte). […]«

II – Faktiske omstændigheder

22. Patrick Breyer har anlagt sag mod Forbundsrepublikken Tyskland med påstand om, at den tilpligtes at undlade at registrere ip-adresser.

23. Talrige tyske forbundsinstitutioner driver offentligt tilgængelige internetportaler, som de stiller aktuelle informationer til rådighed på. Med henblik på at afværge angreb og gøre det muligt at forfølge angriberne strafferetligt foretages der for de fleste af disse internetportalers vedkommende en registrering af alle søgninger i logfiler eller registre. Heri lagres navnet på den konsulterede fil eller websted, begreber, der er blevet indtastet i søgefelter, tidspunktet for søgningen, den overførte mængde data, meldingen om, hvorvidt søgningen lykkedes, og ip-adressen på den computer, der søges fra. Lagringen opretholdes også efter, at den konkrete søgning er afsluttet.

24. Patrick Breyer, som tilgik flere af de nævnte websteder, har i sit søgsmål nedlagt påstand om, at Forbundsrepublikken Tyskland tilpligtes at undlade selv eller gennem tredjemand at registrere ip-adresser på hans værtssystem, der foretager tilkoblingen til webstederne, medmindre registreringen er nødvendig for at kunne genetablere adgangen til telekommunikationstjenesten efter et funktionssvigt.

7 — Lov af 20.12.1990 (BGBl 1990 I, s. 2954).

25. Patrick Breyers søgsmål blev forkastet i første instans. Han fik imidlertid delvis medhold i appelsagen, hvor Forbundsrepublikken Tyskland blev tilpligtet at ophøre med at registrere, efter at den konkrete tilslutning er afsluttet. Kravet om at bringe registreringen til ophør var betinget af, at sagsøgeren i forbindelse med tilslutningen afslører sine personoplysninger, herunder en e-mailadresse, og for så vidt som registreringen ikke er nødvendig for at kunne genetablere adgangen til telekommunikationstjenesten.

III – De forelagte spørgsmål

26. Begge parter har iværksat kassationsanke til prøvelse af dommen, og Bundesgerichtshofs (forbundsdomstolens) VI afdeling for civile sager har forelagt følgende præjudicielle spørgsmål, som indgik til Domstolen den 17. december 2014:

»1) Skal artikel 2, litra a), i Europa-Parlamentets og Rådets direktiv 95/46/EF [...] fortolkes således, at en internetprotokol-adresse (ip-adresse), som en tjenesteudbyder lagrer i forbindelse med en søgning på dennes websted, allerede udgør en personoplysning for tjenesteudbyderens vedkommende, hvis en tredjemand (her: internetudbyder) råder over den yderligere viden, der kræves for at kunne identificere den pågældende person?

2) Er databeskyttelsesdirektivets artikel 7, litra f), til hinder for en bestemmelse i national ret, hvorefter internetudbyderen kun må indsamle og anvende personoplysninger om en bruger uden samtykke fra denne, i det omfang dette er nødvendigt for at kunne afregne og give den pågældende bruger adgang til konkret at benytte telekommunikationstjenesten, og hvorefter formålet om at sikre telekommunikationstjenestens generelle funktionsdygtighed ikke kan begrunde, at personoplysningerne anvendes, også efter at brugeren har afsluttet sin konkrete søgning på webstedet?«

27. Ifølge den forelæggende ret kan sagsøgeren i henhold til tysk lov kræve, at registreringen af ip-adresser ophører, såfremt denne registrering, i overensstemmelse med lovgivningen om beskyttelse af personoplysninger, udgør et ulovligt indgreb i sagsøgerens generelle ret til privatliv – her forstået som selvbestemmelsesretten med hensyn til personlige oplysninger (Bürgerliches Gesetzbuchs (den tyske civillovbog) § 1004, stk. 1, og § 823, stk. 1, sammenholdt med § 1 og § 2 i Grundgesetz (den tyske grundlov).

28. Dette ville være tilfældet, hvis a) ip-adressen (i hvert fald sammen med det tidspunkt, hvor et websted konsulteres) kan klassificeres som »personoplysninger« i henhold til artikel 2, litra a), sammenholdt med 26. betragtning, andet punktum, til direktiv 95/46 og TMG's § 12, stk. 1 og 3, sammenholdt med BDSG's § 3, stk. 1, og b) en lagring ikke er tilladt i henhold til artikel 7, litra f), i direktiv 95/46 eller TMG's § 12, stk. 1 og 3, eller § 15, stk. 1 og 4.

29. For at kunne fortolke den nationale lovgivning (TMG's § 12, stk. 1) er det ifølge Bundesgerichtshof (forbundsdomstol) afgørende at vide, hvordan den personlige karakter af de i artikel 2, litra a), i direktiv 95/46 nævnte oplysninger skal fortolkes.

30. Den forelæggende ret har desuden påpeget, at fortolkningen af TMG's § 15, stk. 1, i henhold til hvilken tjenesteudbyderen kun må indsamle og anvende personoplysninger om en bruger, for så vidt som dette er nødvendigt for at give adgang til telekommunikationstjenester og afregne herfor (data om brugen) [8], er knyttet til fortolkningen af artikel 7, litra f), i direktiv 95/46.

8 — Ifølge Bundesgerichtshof (forbundsdomstol) består data om brugen af specifikationer til identificering af brugeren, oplysninger om påbegyndelse, afslutning og omfanget af den pågældende brug samt oplysninger om de telekommunikationstjenester, som brugeren har anvendt.

IV – Retsforhandlingerne ved Domstolen. Parternes anbringender

31. Den tyske, østrigske og portugisiske regering og Kommissionen har afgivet skriftlige indlæg. Kun Kommissionen og Patrick Breyer deltog i retsmødet den 25. februar 2016. Den tyske regering valgte ikke at deltage.

A – *Parternes anbringender for så vidt angår det første spørgsmål*

32. Ifølge Patrick Breyer er personoplysninger også oplysninger, som kun teoretisk set kan kombineres, dvs. på baggrund af en abstrakt potentiel fare. Det er uvæsentligt, om denne kombination sker i praksis. Efter Patrick Breyers opfattelse betyder den omstændighed, at et organ kan have relativt vanskeligt ved at identificere en person på grundlag af ip-adressen, ikke, at denne person ikke er i fare. Desuden er det efter Patrick Breyers opfattelse relevant, at Tyskland lagrer hans ip-oplysninger for eventuelt at identificere potentielle angreb eller træffe strafferetlige foranstaltninger i henhold til TMG's § 113, hvilket er sket i adskillige tilfælde.

33. Ifølge den tyske regering bør det første spørgsmål besvares benægtende. Efter dens opfattelse afslører dynamiske ip-adresser ikke en »identificeret« person i henhold til artikel 2, litra a), i direktiv 95/46/EF. For at afgøre, om de angiver oplysninger om en »identificerbar« person i henhold til samme bestemmelse, bør *identificerbarheden* undersøges på baggrund af et »subjektivt« kriterium. Dette følger efter den tyske regerings opfattelse af 26. betragtning til direktiv 95/46, i henhold til hvilken der kun skal tages højde for de hjælpemidler, der »med rimelighed« kan tænkes bragt i anvendelse for at identificere den pågældende enten af den registeransvarlige eller af enhver anden person. En sådan præcisering tyder på, at EU-lovgiver ikke har ønsket at lade situationer, hvor det er objektivt muligt for tredjemand at foretage identificering, omfatte af anvendelsesområdet for direktiv 95/46.

34. Den tyske regering har endvidere anført, at begrebet »personoplysninger« som omhandlet i artikel 2, litra a), i direktiv 95/46 bør fortolkes i betragtning af formålet med direktivet, dvs. at sikre overholdelse af de grundlæggende rettigheder. Behovet for at beskytte fysiske personer kan betragtes på en anden måde afhængig af, hvem der er i besiddelse af oplysningerne, og hvorvidt de råder over de nødvendige hjælpemidler til at anvende dem til at identificere disse personer.

35. Den tyske regering har gjort gældende, at Patrick Breyer ikke er identificerbar på grundlag af ip-adresserne sammenholdt med de andre oplysninger, som udbyderne af indhold lagrer. Hertil mangler de oplysninger, som internetudbyderne er i besiddelse af, og som disse udbydere ikke har hjemmel til at videregive til udbyderne af indhold.

36. Den østrigske regering er imidlertid af den opfattelse, at det første spørgsmål bør besvares bekræftende. I overensstemmelse med 26. betragtning til direktiv 95/46 kræves det ikke for at afgøre, om en person er identificerbar, at ét enkelt organ råder over alle specifikationer til identificering af ham. Dermed kan en ip-adresse være en personoplysning, hvis tredjemand (f.eks. en internetudbyder) råder over hjælpemidler til at identificere indehaveren af denne adresse uden at gøre sig uforholdsmæssigt store anstrengelser.

37. Den portugisiske regering er ligeledes fortaler for et bekræftende svar og mener, at ip-adressen – kombineret med datoen for besøget – udgør en personoplysning, for så vidt som dette kan føre til, at en anden enhed end den, der har lagret ip-adressen, kan identificere brugeren.

38. Kommissionen er ligeledes af den opfattelse, at spørgsmålet skal besvares bekræftende, og støtter sig på Domstolens løsning i Scarlet Extended-dommen [9]. Eftersom lagring af ip-adresser netop har til formål at identificere brugere i tilfælde af cyberangreb, udgør anvendelsen af de supplerende oplysninger, som internetudbyderne registrerer, ifølge Kommissionen et hjælpemiddel, som »med rimelighed« kan anvendes som omhandlet i 26. betragtning til direktiv 95/46. Efter Kommissionens opfattelse taler såvel formålet med dette direktiv som artikel 7 og 8 i Den Europæiske Unions charter om grundlæggende rettigheder (herefter »chartret«) for en bred fortolkning af artikel 2, litra a), i direktiv 95/46.

B – *Parternes anbringender for så vidt angår det andet spørgsmål*

39. Patrick Breyer har gjort gældende, at artikel 7, litra f), i direktiv 95/46 udgør en generel bestemmelse, som kræver præcisering for at kunne anvendes. I overensstemmelse med Domstolens praksis drejer det sig dermed om at vurdere den konkrete sags nærmere omstændigheder og afgøre, om der er grupper med en legitim interesse som omhandlet i den pågældende bestemmelse, hvor det ikke blot er tilladt, men påkrævet at opstille specifikke regler for disse grupper med henblik på anvendelsen af denne artikel. I dette tilfælde er den nationale lovgivning ifølge Patrick Breyer forenelig med artikel 7, litra f), i direktiv 95/46, eftersom den offentlige portal ikke har interesse i at lagre personoplysninger, eller fordi beskyttelsen af anonymiteten vejer tungere. Efter hans opfattelse er en systematisk lagring af personoplysninger ikke desto mindre hverken forenelig med et demokratisk samfund, nødvendig eller forholdsmæssig for at sikre de elektroniske mediers funktion, hvilket er fuldt ud muligt uden registrering af personoplysninger, hvilket visse forbundsministeriers websteder har vist.

40. Den tyske regering har gjort gældende, at der ikke er grundlag for at behandle det andet spørgsmål, som udelukkende forelægges i tilfælde af, at det første spørgsmål bør besvares bekræftende, hvilket efter dens opfattelse ikke er tilfældet af de førnævnte årsager.

41. Den østrigske regering har foreslået, at dette spørgsmål besvares således, at direktiv 95/46 overordnet set ikke er til hinder for lagring af oplysninger som de i hovedsagen omtvistede, når dette er afgørende for at sikre funktionsdygtigheden af de elektroniske medier. Ifølge denne regering kan en begrænset lagring af ip-adresser, ud over varigheden af besøget på et websted, være lovlig, for så vidt som den respekterer forpligtelsen for den registeransvarlige for personoplysningerne til at iværksætte de foranstaltninger til beskyttelse af disse oplysninger, som påhviler ham i medfør af artikel 17, stk. 1, i direktiv 95/46. Kampen mod cyberangreb kan berettige en undersøgelse af oplysninger vedrørende tidligere angreb, samt at visse ip-adresser nægtes adgang til webstedet. Forholdsmæssigheden af lagringen af oplysninger som de i hovedsagen omhandlede på grundlag af målet om at sikre de elektroniske mediers funktionsdygtighed bør vurderes fra sag til sag i betragtning af de i artikel 6, stk. 1, i direktiv 95/46 nævnte principper.

42. Den portugisiske regering har gjort gældende, at artikel 7, litra f), i direktiv 95/46 ikke er til hinder for de i hovedsagen omhandlede nationale regler, da den tyske lovgiver allerede må have foretaget en afvejning som fastlagt i denne bestemmelse mellem de legitime interesser hos den registeransvarlige for personoplysningerne på den ene side og de grundlæggende rettigheder og frihedsrettigheder for indehaverne af disse oplysninger på den anden side.

43. Ifølge Kommissionen skal den nationale lovgivning, der gennemfører artikel 7, litra f), i direktiv 95/46, definere målene med behandlingen af personoplysninger således, at de er forudsigelige for den berørte privatperson. Efter Kommissionens opfattelse lever den tyske lov ikke op til dette krav, eftersom TMG's § 15, stk. 1, fastlægger, at lagring af ip-adresser er tilladt »for så vidt som dette er nødvendigt for at give adgang til telekommunikationstjenester«.

9 — Dom af 24.11.2011 (C-70/10, EU:C:2011:771, præmis 51).

44. Kommissionen har derfor foreslået, at det andet spørgsmål besvares således, at denne bestemmelse er til hinder for en fortolkning af en national bestemmelse, i henhold til hvilken en offentlig myndighed, der agerer som tjenesteudbyder, kan indsamle og anvende personoplysninger vedrørende en bruger uden dennes samtykke, også selv om det formål, der forfølges, er at sikre det elektroniske mediums generelle funktionsdygtighed, hvis den pågældende nationale bestemmelse ikke fastlægger dette formål på en tilstrækkelig klar og præcis måde.

V – Bedømmelse

A – *Første spørgsmål*

1. Afgrænsning af det forelagte spørgsmål

45. Som Bundesgerichtshofs (forbundsdomstol) har formuleret sit første spørgsmål søger den at skabe klarhed om, hvorvidt en ip-adresse, som anvendes til at få adgang til et websted, udgør en personoplysning [i henhold til artikel 2, litra a), i direktiv 95/46/EF] for den offentlige myndighed, der er indehaver af dette websted, såfremt en internetudbyder råder over den yderligere viden, der kræves for at kunne identificere den pågældende person.

46. Formuleringen af dette spørgsmål er tilstrækkelig præcis til, at det umiddelbart kan udelukke andre spørgsmål, som i teorien kunne opstå for så vidt angår ip-adressernes retlige karakter i forbindelse med beskyttelsen af personoplysninger.

47. For det første nævner Bundesgerichtshof (forbundsdomstol) udelukkende »dynamiske ip-adresser«, dvs. de adresser, der tildeles midlertidigt til enhver netadgang og ændres ved efterfølgende tilslutninger. De adskiller sig dermed fra »faste eller statiske ip-adresser«, der er kendetegnet ved at være uforanderlige og muliggør permanent identificering af den anordning, der er tilsluttet nettet.

48. For det andet antager den forelæggende ret, at udbyderen af webstedet i den foreliggende sag ikke er i stand til – ved hjælp af den dynamiske ip-adresse – at identificere de besøgende på dennes websteder og desuden ikke selv råder over yderligere viden, der, sammenholdt med den pågældende ip-adresse, gør det muligt at identificere dem. Bundesgerichtshof (forbundsdomstol) forekommer at være af den opfattelse, at den dynamiske ip-adresse i denne forbindelse ikke er en personoplysning i henhold til artikel 2, litra a), i direktiv 95/46 *for udbyderen af webstedet*.

49. Den forelæggende rets tvivl vedrører muligheden for, at den dynamiske ip-adresse klassificeres som en personoplysning for udbyderen af webstedet, *hvis tredjemand råder over yderligere viden*, som, sammenholdt med den dynamiske ip-adresse, identificerer webstedets besøgende. Endnu en relevant præcisering er, at Bundesgerichtshof (forbundsdomstol) ikke refererer til en hvilken som helst tredjemand, som råder over yderligere viden, men derimod udelukkende til internetudbyderen (og dermed udelukker andre mulige indehavere af denne type oplysninger).

50. Følgende er dermed ikke omfattet af debatten: a) hvorvidt statiske ip-adresser er personoplysninger i henhold til direktiv 95/46 [10], b) hvorvidt dynamiske ip-adresser altid og under alle omstændigheder er personoplysninger i henhold til dette direktiv, og endelig c) hvorvidt klassificeringen af dynamiske ip-adresser som personoplysninger er uundgåelig, så snart der findes en tredjepart, uanset hvem dette er, som kan anvende de dynamiske ip-adresser til at identificere brugere af nettet.

51. Det drejer sig dermed udelukkende om at afgøre, om en dynamisk ip-adresse er en personoplysning for en udbyder af en internettjeneste, når den virksomhed, der udbyder adgang til nettet (internetudbyderen), råder over yderligere viden, som, kombineret med denne adresse, gør det muligt at identificere, hvem der besøger det websted, der forvaltes af førstnævnte.

2. Om realiteten

52. Det spørgsmål, der rejses i denne forelæggelse, er genstand for en intens debat i retslitteraturen og i tysk retspraksis, hvor der er opstået to fløje [11]. Ifølge den ene fløj (som er fortaler for et »objektivt« eller »absolut« kriterium) er en bruger identificerbar – og ip-adressen er dermed en personoplysning, der kan beskyttes – når, uanset udbyderen af internettjenestens kundskaber eller hjælpemidler, brugeren kan identificeres ved blot at sammenholde denne dynamiske ip-adresse med de af tredjemand afgivne oplysninger (f.eks. internetudbyderen).

53. Ifølge den anden fløj (som taler for et »subjektivt« kriterium) er muligheden for at gøre brug af tredjemands hjælp i forbindelse med den endelige identificering af brugeren ikke tilstrækkelig til at tillægge dynamiske ip-adresser personlig karakter. Det relevante er evnen hos den, der har adgang til oplysningen, til at gøre brug af den med egne midler og herved identificere en person.

54. Uanset denne strids nærmere omstændigheder i den nationale lovgivning bør Domstolens svar være begrænset til en fortolkning af de to bestemmelser i direktiv 95/46, som både den forelæggende ret og sagens parter har henvist til, altså artikel 2, litra a) [12], og 26. betragtning [13].

55. Blot den omstændighed, at dynamiske ip-adresser indeholder oplysninger om datoen og tidspunktet for, hvornår en computer (eller en anden anordning) har besøgt et websted, afslører de visse mønstre for internetbrugernes adfærd, og dermed udgør de en mulig overtrædelse af deres ret til respekt for deres privatliv [14], som er garanteret ved artikel 8 i den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder og ved chartrets artikel 7, henset til hvilke – samt chartrets artikel 8 – direktiv 95/46 skal fortolkes [15]. Sagens parter stiller ikke spørgsmål ved denne præmis, der heller ikke som sådan er genstand for det præjudicielle spørgsmål.

10 — Domstolen tog stilling til dette problem i dom af 24.11.2011, Scarlet Extended (C-70/10, EU:C:2011:771, præmis 51), og af 19.4.2012, Bonnier Audio m.fl. (C-461/10, EU:C:2012:219). I præmis 51 og 52 i sidstnævnte dom konkluderede Domstolen, at udlevering af oplysninger »med det formål at kunne identificere en internetabonnent eller -bruger, der benytter den ip-adresse, som angiveligt blev anvendt til den ulovlige fildeling af de beskyttede værker, [...] om navn og adresse på denne abonnent eller bruger [...] udgør en behandling af personoplysninger i henhold til artikel 2, stk. 1, i direktiv 2002/58, sammenholdt med artikel 2, litra b), i direktiv 95/46«.

11 — Vedrørende de to opfattelser i retslitteraturen, jf. f.eks. M. Schreibauer, i *Kommentar zum Bundesdatenschutzgesetz. Nebengesetze*, M. Esser, P. Kramer og K. von Lewinski. (red.), Carl Heymanns Verlag/Wolters Kluwer, Køln, 2014, 4. udg., § 11 Telemediengesetz (4-10). J. Nink og J. Pohle: »Die Bestimmbarkeit des Personenbezugs. Von der IP-Adresse zum Anwendungsbereich der Datenschutzgesetze«, i *Multimedia und Recht*, 9/2015, s. 563-567. J. Heidrich og C. Wegener: »Rechtliche und technische Anforderungen an die Protokollierung von IT-Daten. Problemfall Logging«, i *Multimedia und Recht*, 8/2015, s. 487-492. H. Leisterer: »Die neuen Pflichten zur Netz– und Informationssicherheit und die Verarbeitung personenbezogener Daten zur Gefahrenabwehr«, i *Computer und Recht*, 10/2015, s. 665-670.

12 — Gengivet i punkt 13.

13 — Gengivet i punkt 11.

14 — Således formulerede generaladvokat Cruz Villalón det i sit forslag til afgørelse Scarlet Extended (C-70/10, EU:C:2011:255, punkt 76), og Den Europæiske Tilsynsførende for Databeskyttelse var af samme opfattelse i sin udtalelse af 22.2.2010 om Den Europæiske Unions forhandlinger om en handelsaftale vedrørende bekæmpelse af forfalskning (ACTA) (EUT 2010, C 147, s. 1, præmis 24) og udtalelse af 10.5.2010 om forslaget til Europa-Parlamentets og Rådets direktiv om bekæmpelse af seksuelt misbrug af børn, seksuel udnyttelse af børn og børnepornografi og om ophævelse af rammeafgørelse 2004/68/RIA (EUT 2010, C 323, s. 6, præmis 11).

15 — Jf. i denne forbindelse dom af 20.5.2003, Österreichischer Rundfunk (C-465/00, C-138/01 og C-139/01, EU:C:2003:294, præmis 68), og generaladvokat Kokotts forslag til afgørelse Promusicae (C-275/06, EU:C:2007:454, punkt 51 ff.).

56. Den person, som disse detaljer vedrører, er ikke en »identificeret fysisk person«. Datoen og tidspunktet for en forbindelse, samt den numeriske adresse, hvorfra forbindelsen oprettes, afslører hverken direkte eller indirekte identiteten på den fysiske person, som ejer den anordning, hvorfra webstedet besøges, eller identiteten på den bruger, som anvender den (det kan være en hvilken som helst fysisk person).

57. For så vidt som en dynamisk ip-adresse bidrager til at identificere – enten i sig selv eller kombineret med andre oplysninger – ejeren af den anordning, der anvendes til at besøge webstedet, kan den imidlertid klassificeres som en oplysning om en »identificerbar person« [16].

58. Ifølge Bundesgerichtshof (forbundsdomstol) er en dynamisk ip-adresse i sig selv ikke tilstrækkelig til at identificere den bruger, som ved hjælp af denne adresse har besøgt et websted. Hvis udbyderen af internettjenesten derimod ved hjælp af den dynamiske ip-adresse kunne identificere brugeren, ville der uden tvivl være tale om en personoplysning i henhold til direktiv 95/46. Dette forekommer imidlertid ikke at være betydningen af det præjudicielle spørgsmål, hvori det er underforstået, at udbyderne af internettjenester, der er omfattet af tvisten i hovedsagen, ikke kan identificere brugeren udelukkende ved hjælp af den dynamiske ip-adresse.

59. Den dynamiske ip-adresse, sammenholdt med andre oplysninger, gør det muligt »indirekte« at identificere brugeren, hvilket alle parterne er enige om. Kan muligheden for, at der foreligger yderligere oplysninger, der kan knyttes til den dynamiske ip-adresse, uden videre begrunde, at sidstnævnte klassificeres som en personoplysning i henhold til direktivet? Det må i denne forbindelse afgøres, om den blotte teoretiske mulighed for at få kendskab til disse oplysninger er tilstrækkelig, eller om det derimod er afgørende, at de er tilgængelige for den, der har kendskab til den dynamiske ip-adresse, eller for tredjemand.

60. Parterne har koncentreret deres bemærkninger om fortolkningen af 26. betragtning til direktiv 95/46. Her har de fremhævet formuleringen »hjælpemidler [...], der med rimelighed kan tænkes bragt i anvendelse for at identificere den pågældende enten af den registeransvarlige eller af enhver anden person«. Den forelæggende rets spørgsmål vedrører ikke yderligere oplysninger, som de tjenesteudbydere, der er omfattet af hovedsagen, råder over. Det henviser heller ikke til enhver tredjemand, der måtte råde over disse yderligere oplysninger (der sammenholdt med den dynamiske ip-adresse gør det muligt at identificere brugeren), men derimod til internetudbyderen.

61. Det er dermed ikke nødvendigt, at Domstolen i denne sag undersøger alle de hjælpemidler, som den sagsøgte i hovedsagen »med rimelighed« kunne anvende, for at de dynamiske ip-adresser, som denne er i besiddelse af, kan klassificeres som personoplysninger. Eftersom Bundesgerichtshof (forbundsdomstol) udelukkende nævner yderligere oplysninger, som tredjemand råder over, kan det udledes: a) enten at sagsøgte ikke selv råder over yderligere oplysninger, der gør det muligt at identificere brugeren, b) eller, såfremt han råder over disse oplysninger, at han ikke er i stand til at anvende dem med rimelighed til dette formål i sin egenskab af registeransvarlig i henhold til 26. betragtning til direktiv 95/46.

16 — Medmindre andet kan dokumenteres, bør det antages, at dette er den person, der har benyttet internettet og besøgt det pågældende websted. Ses der bort fra sidstnævnte antagelse, giver oplysninger om dato og tidspunkt for en forbindelse samt den numeriske adresse, hvorfra forbindelsen oprettes, i forbindelse med et besøg af et websted stadig mulighed for at knytte dette besøg til indehaveren af anordningen og indirekte associere ham med mønstrene for hans adfærd på nettet. En mulig undtagelse kunne være ip-adresser, der tildeles computere på f.eks. netcaféer, hvis anonyme brugere ikke er identificerbare, og den trafik, der genereres i lokalerne, ikke afslører nogen relevante personoplysninger. Dette er desuden den eneste undtagelse til princippet om, at ip-adresser er personoplysninger, der er anerkendt af gruppen til beskyttelse af personer i forbindelse med behandling af personoplysninger, som er oprettet ved direktiv 95/46 (den såkaldte »artikel 29-gruppe«). Jf. gruppens udtalelse nr. 4/2007 af 20.6.2007 om begrebet personoplysninger, WP 136, som er tilgængelig på adressen http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

62. Begge muligheder afhænger af en konstatering de faktiske omstændigheder, som det udelukkende tilkommer den forelæggende ret at foretage. Domstolen kan bibringe den generelle kriterier med henblik på fortolkningen af formuleringen »hjælpemidler [...], der med rimelighed kan tænkes bragt i anvendelse [...] af den registeransvarlige«, såfremt Bundesgerichtshof (forbundsdomstol) er i tvivl om, hvorvidt sagsøgte er i stand til med rimelighed at anvende sine egne yderligere oplysninger. Eftersom dette ikke er tilfældet, ville det efter min opfattelse være forkert af Domstolen at fastlægge fortolkningskriterier, som ikke er afgørende for den forelæggende ret, som desuden ikke har anmodet herom.

63. Det forelagte spørgsmål drejer sig dermed grundlæggende om at afgøre, om det for at klassificere dynamiske ip-adresser som personoplysninger er relevant, at en yderst specifik tredjemand – internetudbyderen – råder over yderligere oplysninger, som, sammenholdt med disse adresser, gør det muligt at identificere den bruger, der har besøgt et bestemt websted.

64. Det er atter nødvendigt at henvise til 26. betragtning til direktiv 95/46. Formuleringen »hjælpemidler [...], der med rimelighed kan tænkes bragt i anvendelse [...] *af enhver anden person*« [17], kunne danne grundlag for en fortolkning, hvorefter det er tilstrækkeligt, at tredjemand kan opnå yderligere oplysninger (der kan sammenholdes med en dynamisk ip-adresse med henblik på at identificere en person), således at denne adresse anses for at udgøre en personoplysning *eo ipso*.

65. Denne maksimalistiske fortolkning ville i praksis føre til, at alle former for information ville blive klassificeret som personoplysninger, uanset hvor lidet brugbar den måtte være i forbindelse med identificeringen af en bruger. Det kan aldrig med 100% sikkerhed fastslås, at der ikke er en tredjemand, der er i besiddelse af yderligere oplysninger, der kan kombineres med denne viden, og som dermed kan anvendes til at afsløre identiteten på en person.

66. Muligheden for, at udviklingen i tekniske hjælpemidler i mere eller mindre nær fremtid væsentligt letter adgangen til mere og mere sofistikerede instrumenter, der kan indsamle og behandle oplysninger, begrunder efter min opfattelse de forholdsregler, der har til formål at beskytte privatlivets fred. I forbindelse med definitionen af de relevante juridiske kategorier inden for databeskyttelse er der blevet gjort bestræbelser på at inkludere faktiske scenarier, der er tilstrækkeligt brede og fleksible, således at dækningen omfatter enhver tænkelig situation [18].

67. Denne bekymring, som i øvrigt er meget berettiget, kan efter min opfattelse imidlertid ikke medføre en tilsidesættelse af lovgivers hensigt, eller at den systematiske fortolkning af 26. betragtning til direktiv 95/46 begrænses til »de hjælpemidler [...], der med rimelighed kan tænkes bragt i anvendelse« *af visse tredjemænd*.

68. Ligesom 26. betragtning ikke henviser til alle mulige hjælpemidler, der kan tænkes bragt i anvendelse af den registeransvarlige (udbyderen af internettjenester i dette tilfælde), men derimod blot til de hjælpemidler, som denne »med rimelighed« kan anvende, skal det også forstås således, at lovgiver henviser til »tredjemænd«, som den registeransvarlige, der søger at indhente yderligere oplysninger med henblik på identificering, *ligeledes med rimelighed*, kan henvende sig til. Dette er ikke tilfældet, når kontakten med disse tredjemænd i praksis kræver omfattende menneskelige og økonomiske ressourcer eller er uigennemførlige eller ulovlige. Som jeg tidligere har nævnt, ville det i modsat fald

17 — Min fremhævelse.

18 — Dette mål om forsigtighed og forebyggelse er baseret på artikel 29-gruppens holdning. Som jeg har nævnt, bør udgangspunktet ifølge gruppen være, at ip-adresser udgør personoplysninger, og at den eneste undtagelse hertil bør være tilfælde, hvor tjenesteudbyderen er i stand til med 100% sikkerhed at fastslå, at oplysningerne vedrører brugere, der ikke kan identificeres, som f.eks. brugere af en netcafé. Jf. fodnote 16, in fine.

være praktisk umuligt at sondre mellem hjælpemidlerne, idet det altid vil være muligt at forestille sig en tredjemand, der, uanset hvor utilgængelig denne måtte være for udbyderen af internettjenester – nu eller i fremtiden – kan råde over yderligere oplysninger, der kan bidrage til identificeringen af en bruger.

69. Som nævnt er den af Bundesgerichtshof (forbundsdomstol) nævnte tredjemand en internetudbyder. Her er uden tvivl tale om den tredjemand, som tjenesteudbyderen med størst sandsynlighed vil henvende sig til for at indhente de nærmere yderligere oplysninger, hvis denne søger en mere effektiv, praktisk og direkte identificering af den bruger, der har besøgt dennes websted, ved hjælp af den dynamiske ip-adresse. Der er på ingen måde tale om en hypotetisk tredjemand, men derimod en central aktør på internettet, som med sikkerhed råder over de oplysninger, som tjenesteudbyderen behøver for at kunne identificere en bruger. Således som den forelæggende ret har anført, har den sagsøgte i hovedsagen til hensigt at henvende sig til netop denne tredjemand for at indhente de for sagsøgte nødvendige oplysninger.

70. Internetudbyderen er normalt den tredjemand, som 26. betragtning til direktiv 95/46 henviser til som den, som tjenesteudbyderen i den pågældende sag med størst »rimelighed« kan henvende sig til. Det bør imidlertid tydeliggøres, om indhentningen af de yderligere oplysninger, som denne tredjemand råder over, »med rimelighed« kan anses for at være praktisk mulig eller gennemførlig.

71. Den tyske regering har gjort gældende, at eftersom de oplysninger, som internetudbyderen råder over, udgør personoplysninger, kan denne ikke videregive dem uden videre, medmindre dette sker i overensstemmelse med lovgivningen om behandling af sådanne oplysninger [19].

72. Det forholder sig utvivlsomt således, eftersom det for at kunne drage fordel af disse oplysninger er nødvendigt at overholde den gældende lovgivning vedrørende personoplysninger. Oplysninger kan kun indhentes »med rimelighed«, hvis betingelserne for adgang til denne type oplysninger er opfyldt, hvilket først og fremmest indebærer, at det skal være lovligt muligt at lagre og videregive oplysningerne til andre. Det er korrekt, at internetudbyderen kan afvise at videregive de pågældende oplysninger, men det modsatte kan også gøre sig gældende. En fuldstændig »rimelig« mulighed for at videregive oplysninger medfører i sig selv, at den dynamiske ip-adresse bliver en personoplysning for udbyderen af internettjenester i overensstemmelse med kriterierne i 26. betragtning til direktiv 95/46.

73. Der er tale om en mulighed *inden for lovens rammer*, som dermed er »rimelig«. De rimelige hjælpemidler til adgang, som direktiv 95/46 henviser til, må dermed pr. definition være lovlige hjælpemidler [20]. Dette er den præmis, som den forelæggende ret ganske naturligt tager udgangspunkt i, hvilket den tyske regering har bemærket [21]. Dermed begrænses de juridisk relevante adgangsmuligheder i væsentlig grad, eftersom udelukkende lovlige muligheder kan anvendes. Så længe disse findes, uanset hvor restriktive de måtte være for så vidt angår den praktiske anvendelse, udgør de »rimelige hjælpemidler« som omhandlet i direktiv 95/46.

74. Som følge heraf er det min opfattelse, at det første af de af Bundesgerichtshofs (forbundsdomstol) forelagte spørgsmål, således som det er affattet, bør besvares bekræftende. Den dynamiske ip-adresse bør for udbyderen af internettjenester kategoriseres som en personoplysning, henset til, at der findes en tredjemand (internetudbyderen), som førstnævnte med rimelighed kan henvende sig til for at indhente andre yderligere oplysninger, som – sammenholdt med den dynamiske ip-adresse – kan gøre det muligt at identificere en bruger.

19 — Punkt 40 og 45 i den tyske regerings skriftlige indlæg.

20 — I denne forbindelse er det irrelevant, at det i praksis er muligt at få adgang til personoplysningen ved at tilsidesætte databeskyttelseslovene.

21 — Punkt 47 og 48 i den tyske regerings skriftlige indlæg.

75. Det resultat, der ville følge af et andet svar end det, som jeg foreslår, understøtter efter min opfattelse dette svar. Hvis de dynamiske ip-adresser ikke udgør en personoplysning for udbyderen af internettjenester, kan denne lagre dem på ubestemt tid og når som helst anmode internetudbyderen om de yderligere oplysninger med henblik på at sammenholde disse med de dynamiske ip-adresser og identificere brugeren. Som den tyske regering har medgivet, vil den dynamiske ip-adresse under disse omstændigheder være en personoplysning, eftersom de yderligere oplysninger til identificering af brugeren allerede foreligger, hvilket betyder, at databeskyttelseslovgivningen finder anvendelse [22].

76. Der vil være tale om en oplysning, hvis lagring udelukkende vil være mulig, for så vidt som den fra det pågældende tidspunkt ikke er blevet klassificeret som en personoplysning for tjenesteudbyderen. Den retlige klassificering af den dynamiske ip-adresse som personoplysning vil dermed være op til tjenesteudbyderen og være betinget af muligheden for, at denne på et senere tidspunkt vælger at anvende den til at identificere en bruger ved at sammenholde den dynamiske ip-adresse med de andre yderligere oplysninger, som skal indhentes hos tredjemand. Det afgørende er efter min opfattelse derimod den – rimelige – mulighed i henhold til direktiv 95/46 for, at der findes en »tilgængelig« tredjemand, der råder over de nødvendige hjælpemidler til at muliggøre identificering af en person, og ikke muligheden for, at der sker henvendelse til denne tredjemand.

77. Ifølge den tyske regering kunne det ligeledes medgives, at den dynamiske ip-adresse først bliver en personoplysning, så snart internetudbyderen modtager den. Det skulle imidlertid accepteres, at denne klassificering anvendes med tilbagevirkende kraft for så vidt angår opbevaringsperioden for ip-adressen, og at ip-adressen dermed betragtes som ikke-eksisterende, hvis den er blevet opbevaret ud over det tidsrum, der er tilladt, såfremt den fra første færd er blevet klassificeret som en personoplysning. Ifølge denne tilgang vil man nå til et resultat, der er i strid med ånden i databeskyttelseslovgivningen. Begrundelsen for en blot midlertidig lagring af disse oplysninger vil blive undermineret af enhver forsinkelse i fastlæggelsen af relevansen af et karaktertræk, som gør sig gældende for oplysningerne fra begyndelsen: deres potentiale som et hjælpemiddel til identificering – i sig selv eller sammenholdt med andre oplysninger – af en fysisk person. Det er ligeledes af denne udelukkende økonomiske årsag mere rimeligt at tillægge oplysningerne denne egenskab fra begyndelsen.

78. Dermed er det min opfattelse, som en første konklusion, at artikel 2, litra a), i direktiv 95/46/EF skal fortolkes således, at en ip-adresse, som en tjenesteudbyder lagrer i forbindelse med et besøg på dennes websted, udgør en personoplysning for tjenesteudbyderens vedkommende, for så vidt som en (inter)netudbyder råder over den yderligere viden, der kræves for at kunne identificere den pågældende person.

B – *Det andet spørgsmål*

79. Med det andet præjudicielle spørgsmål ønsker Bundesgerichtshof (forbundsdomstol) oplyst, hvorvidt artikel 7, litra f), i direktiv 95/46 er til hinder for en bestemmelse i national ret, hvorefter der kun må indsamles og anvendes personoplysninger om en bruger uden samtykke fra denne, for så vidt som dette er nødvendigt for at kunne afregne og give den pågældende bruger adgang til konkret at benytte tjenesten, og hvorefter formålet om at sikre telekommunikationstjenestens generelle funktionsdygtighed ikke kan begrunde, at disse oplysninger anvendes, når hvert enkelt besøg er afsluttet.

80. Forud for svaret bør der ske en præcisering af de af Bundesgerichtshof (forbundsdomstol) forelagte oplysninger, i henhold til hvilke de omstridte oplysninger lagres for at sikre den generelle funktionsdygtighed af de i hovedsagen omhandlede websteder, hvilket muliggør en strafferetlig forfølgelse af eventuelle cyberangreb, som webstederne kan være genstand for.

22 — Punkt 36 i den tyske regerings skriftlige indlæg.

81. Det skal dermed først og fremmest undersøges, hvorvidt behandlingen af de af forelæggelsen omfattede ip-adresser er omfattet af undtagelsen i artikel 3, stk. 2, første led, i direktiv 95/46 [23].

1. Spørgsmålet om anvendelsen af direktiv 95/46 på behandlingen af de omstridte oplysninger

82. I hovedsagen optræder Forbundsrepublikken Tyskland tilsyneladende blot som en udbyder af internettjenester, dvs. som en privatperson (og dermed sine imperio). På denne baggrund kan det konkluderes, at behandlingen af de af denne sag omfattede oplysninger i princippet ikke er undtaget fra anvendelsesområdet for direktiv 95/46.

83. Som Domstolen konstaterede i Lindqvist-dommen [24], er aktiviteterne i artikel 3, stk. 2, i direktiv 95/46 »under alle omstændigheder statens eller statslige myndigheders aktiviteter og har ikke noget at gøre med området for den enkelte borgers aktiviteter« [25]. For så vidt som behandlingen af de omstridte oplysninger varetages af en registeransvarlig, der på trods af sin egenskab af offentlig myndighed i realiteten optræder som en privatperson, finder direktiv 95/46 anvendelse.

84. Den forelæggende ret har fremhævet, at det hovedformål, som de tyske myndigheder forfølger med registreringen af de dynamiske ip-adresser, er at »garantere og opretholde sikkerheden og funktionsdygtigheden af deres telekommunikationstjeneste« ved navnlig at fremme »identifikation og afværgelse af de hyppigt forekommende »Denial-of-Service«-angreb, hvorved telekommunikationsinfrastrukturen lammes, idet enkelte webservere målrettet og koordineret oversvømmes med en stor mængde anmodninger« [26]. Enhver indehaver af websteder af en vis betydning opbevarer som regel dynamiske ip-adresser af denne årsag, hvilket hverken direkte eller indirekte indebærer udøvelse af offentlig myndighed, og dermed kan denne opbevaring omfattes af anvendelsesområdet for direktiv 95/46 uden uforholdsmæssigt store vanskeligheder.

85. Bundesgerichtshof (forbundsdomstol) har imidlertid gjort gældende, at de i hovedsagen omhandlede tjenesteudbyderes opbevaring af dynamiske ip-adresser ligeledes skyldes et formål om at forfølge bagmændene bag eventuelle cyberangreb strafferetligt. Er dette formål tilstrækkeligt til at udelukke behandlingen af disse oplysninger fra anvendelsesområdet for direktiv 95/46?

86. Hvis der ved »strafferetlige foranstaltninger« skal forstås de i hovedsagen sagsøgte tjenesteudbyderes udøvelse af statens straffebeføjelser, omhandler denne sag efter min opfattelse en af »statens aktiviteter på det strafferetlige område« og dermed en af undtagelserne i artikel 3, stk. 2, første led, i direktiv 95/46.

87. Under disse omstændigheder følger det af Domstolens praksis i Huber-dommen [27], at tjenesteudbydernes behandling af personoplysninger med henblik på sikkerheden og funktionsdygtigheden af deres telekommunikationstjeneste er omfattet af anvendelsesområdet for direktiv 95/46, mens behandlingen af oplysninger med henblik på statens aktiviteter på det strafferetlige område falder uden for dette anvendelsesområde.

23 — »[B]ehandling, der vedrører den offentlige sikkerhed, forsvar, statens sikkerhed [...] og *statens aktiviteter på det strafferetlige område*« (ikke fremhævet i originalen) er ikke omfattet af anvendelsesområdet for direktiv 95/46.

24 — Dom af 6.11.2003 (C-101/01, EU:C:2003:596, præmis 43).

25 — Jf. i denne forbindelse dom af 16.12.2008, Satakunnan Markkinapörssi og Satamedia (C-73/07, EU:C:2008:727, præmis 41).

26 — Punkt 36 i forelæggelseskendelsen.

27 — Dom af 16.12.2008 (C-524/06, EU:C:2008:724, præmis 45).

88. Selv hvis Forbundsrepublikken Tyskland, som blot agerer som tjenesteudbyder sine imperio, ikke er ansvarlig for gennemførelsen af den strafferetlige foranstaltning i egentlig forstand, men som enhver anden privatperson blot videregiver de omtvistede ip-adresser til et statsligt organ med henblik på håndhævelse, vil behandlingen af de dynamiske ip-adresser ligeledes være rettet mod en aktivitet, der falder uden for anvendelsesområdet for direktiv 95/46.

89. Dette følger af retspraksis i dommen i sagen Parlamentet mod Rådet og Kommissionen [28], hvori Domstolen fastslog, at den omstændighed, at visse personoplysninger »er blevet indsamlet af private erhvervsdrivende til kommercielle formål, og at det er disse erhvervsdrivende, som forestår oplysningernes videregivelse til en tredjestat«, ikke indebærer, at denne videregivelse »ikke er omfattet af [...] anvendelsesområde[t]« for artikel 3, stk. 2, første led, i direktiv 95/46, når formålet med videregivelsen vedrører statens aktiviteter på det strafferetlige område, så længe denne videregivelse »sker [...] inden for rammer, der er indført af de statslige myndigheder, og som vedrører den offentlige sikkerhed« [29].

90. Hvis »strafferetlige foranstaltninger«, som det fremgår af forelæggelseskendelsen, og som jeg mener, således vedrører en privatpersons beføjelse til at iværksætte statens udøvelse af straffebeføjelser ved hjælp af passende foranstaltninger, kan det ikke gøres gældende, at behandlingen af dynamiske ip-adresser er rettet mod statens aktiviteter på det strafferetlige område, som falder uden for anvendelsesområdet for direktiv 95/46.

91. Lagring og registrering af disse oplysninger er endnu et bevis, som indehaveren af webstedet kunne anvende til at anmode staten om retsforfølgning af en ulovlig adfærd. Dette ville netop være et redskab til et strafferetligt forsvar af en privatpersons rettigheder, der er anerkendt i lovgivningen (i dette tilfælde en offentlig myndighed, der agerer på det privatretlige område). I henhold til denne opfattelse er dette ikke forskelligt fra en anden internetudbyder, der søger statslig beskyttelse i henhold til de procedurer for iværksættelse af strafferetlige foranstaltninger, som er fastlagt i lovgivningen.

92. For så vidt som de tyske myndigheder agerer som udbyder af internettjenester, der ikke har offentligretlige beføjelser – hvilket er et spørgsmål, som det tilkommer den forelæggende ret at bedømme – er den behandling, som de foretager af de dynamiske ip-adresser, idet der er tale om personoplysninger, dermed omfattet af anvendelsesområdet for direktiv 95/46.

2. Om realiteten

93. TMG's § 15, stk. 1, tillader kun indsamling og anvendelse af personoplysninger om en bruger, for så vidt som dette er nødvendigt for at kunne afregne og give den pågældende bruger adgang til konkret at benytte telekommunikationstjenesten. Nærmere betegnet må tjenesteudbyderen kun indsamle og anvende de såkaldte »data om brugen«, dvs. personoplysninger om en bruger, for så vidt som dette er nødvendigt for »at give adgang til telekommunikationstjenester og afregne herfor«. I henhold til TMG's § 15, stk. 4, skal disse oplysninger slettes igen, når den pågældende brug er afsluttet (dvs. når den konkrete brug af telekommunikationstjenesten er ophørt), medmindre de er nødvendige »af hensyn til afregningen«.

28 — Dom af 30.5.2006 (C-317/04 og C-318/04, EU:C:2006:346, præmis 54-59).

29 — Ibidem, præmis 59. Sagen omhandlede personoplysninger, hvis behandling ikke var nødvendig for den levering af tjenesteydelser, der udgjorde de berørte private aktørers virksomhed (luftfartsselskaber), men som disse aktører anså sig for at være forpligtede til at videregive til de amerikanske myndigheder for at forebygge og bekæmpe terrorisme.

94. Efter at tilslutningen er ophørt, forekommer TMG's § 15 at udelukke, at dataene om brugen lagres af andre hensyn, heriblandt for generelt at sikre »adgang til telekommunikationstjenester«. Eftersom denne bestemmelse i TMG udelukkende vedrører hensyn til afregning som begrundelse for lagring af oplysningerne, kan denne bestemmelse fortolkes (selv om den endelige fortolkning heraf tilkommer den forelæggende ret) således, at dataene om brugen kun må anvendes til at muliggøre en konkret tilslutning, og at de skal slettes, når denne ophører.

95. Artikel 7, litra f), i direktiv 95/46 [30] tillader behandling af personoplysninger på betingelser, som efter min opfattelse er mere lempelige (for den registeransvarlige) end de betingelser, der fremgår af ordlyden af TMG's § 15. Den tyske bestemmelse kan i dette tilfælde betragtes som værende mere restriktiv end den EU-retlige, idet den som udgangspunkt kun omfatter forfølgelse af legitime interesser, der vedrører afregning for tjenesten, mens Forbundsrepublikken Tyskland, i sin egenskab af udbyder af internettjenester, også kan have en legitim interesse i at sikre funktionsdygtigheden af sine websteder, ud over den enkelte tilslutning [31].

96. Domstolens praksis i dommen i sagen ASNEF og FECEMD [32] udstikker de nødvendige retningslinjer for besvarelsen af det andet præjudicielle spørgsmål. Domstolen konstaterede i denne sag, at det af formålet med direktiv 95/46 »følger [...], at artikel 7 i direktiv 95/46 fastsætter en udtømmende og fuldstændig liste over de tilfælde, hvor behandling af personoplysninger kan anses for at være lovlig« [33]. Heraf følger, »at medlemsstaterne hverken kan tilføje nye principper vedrørende grundlaget for behandling af oplysninger i artikel 7 i direktiv 95/46 eller fastsætte supplerende krav, som ændrer rækkevidden af et af de seks principper, der er fastsat i denne artikel« [34].

97. I forhold til artikel 7 i direktiv 95/46 opstiller TMG's § 15 ikke yderligere betingelser for lovlig behandling af personoplysninger – hvilket var tilfældet i ASNEF og FECEMD-sagen [35] – men den reducerer indholdet af betingelsen i artiklens litra f), såfremt der foretages en restriktiv fortolkning, hvilket den forelæggende ret taler for: Hvor EU-lovgiver generelt henviser til, at »den registeransvarlige eller den tredjemand eller de tredjemænd, til hvem oplysningerne videregives, kan forfølge en legitim interesse«, tager TMG's § 15 kun hensyn til behovet for at »give [konkret] adgang til telekommunikationstjenester og afregne herfor«.

98. Ligesom i ASNEF og FECEMD-sagen [36] ændrer en national foranstaltning i denne sag – såfremt der atter anlægges en restriktiv fortolkning, som der er gjort rede for ovenfor – rækkevidden af et princip i artikel 7 i direktiv 95/46 i stedet for at blot at præcisere denne rækkevidde, hvilket er det eneste, de enkelte medlemsstaters myndigheder har en vis skønsbeføjelse til i henhold til artikel 5 i direktiv 95/46.

30 — Gengivet i punkt 17.

31 — Jf. punkt 84. Indehaverne af webstederne forfølger bestemt en legitim interesse i at forebygge og bekæmpe angreb på tjenesten (»denials of service«), som den forelæggende ret nævner, altså de massive koordinerede angreb, der i visse tilfælde foretages mod nogle websteder for at blokere dem og gøre dem umulige at anvende.

32 — Dom af 24.11.2011 (C-468/10 og C-469/10, EU:C:2011:777).

33 — Ibidem, præmis 30.

34 — Ibidem, præmis 32.

35 — I denne sag supplerede den nationale lovgivning betingelserne i artikel 7, litra f), i direktiv 95/46 med en betingelse om, at de oplysninger, der er genstand for behandlingen, skal fremgå af offentligt tilgængelige kilder.

36 — Dom af 24.11.2011 (C-468/10 og C-469/10, EU:C:2011:777).

99. Ifølge sidstnævnte bestemmelse »[...] præciserer [medlemsstaterne] i henhold til bestemmelserne i dette kapitel [37], på hvilke betingelser behandling af personoplysninger er lovlig«. Således som Domstolen konstaterede i ASNEF og FECEMD-sagen[38] »[kan] medlemsstaterne i medfør af [den pågældende bestemmelse] heller ikke [...] indføre andre principper vedrørende grundlaget for behandling af personoplysninger end dem, der er opregnet i dette direktivs artikel 7, eller ved supplerende krav ændre rækkevidden af de seks principper, der er fastsat i nævnte artikel 7«.

100. I forbindelse med artikel 7, litra f), i direktiv 95/46 begrænser TMG's § 15 i væsentlig grad omfanget af den legitime interesse, der er nødvendig for at begrunde behandlingen af oplysninger, og begrænser sig ikke til at præcisere eller nuancere den inden for rammerne af, hvad der er tilladt i henhold til direktivets artikel 5. Dette gør den desuden eftertrykkeligt og kategorisk uden at anerkende, at beskyttelse og sikring af den generelle adgang til telekommunikationstjenester kan afvejes i forhold til »den registreredes interesser eller de grundlæggende rettigheder og frihedsrettigheder, der skal beskyttes i henhold til artikel 1, stk. 1« i direktiv 95/46 i henhold til direktivets artikel 7, litra f).

101. Ligesom i ASNEF og FECEMD-sagen[39] har den tyske lovgiver »definitivt [foreskrevet] resultatet af afvejningen af de modstående rettigheder og interesser [for bestemte kategorier af personoplysninger], uden at tillade et anderledes resultat som følge af særlige omstændigheder i det konkrete tilfælde«, således, at der »imidlertid ikke længere [er] tale om en præcisering som omhandlet i [...] artikel 5« i direktiv 95/46.

102. Under disse omstændigheder er det min opfattelse, at Bundesgerichtshof (forbundsdomstol) er forpligtet til at fortolke den nationale lovgivning i overensstemmelse med direktiv 95/46, hvilket indebærer: a) at begrundelser for behandlingen af de såkaldte »data om brugen« kan omfatte den legitime interesse hos udbyderen af telekommunikationstjenester i at beskytte den generelle adgang hertil, og b) at denne interesse hos tjenesteudbyderen i de enkelte tilfælde kan afvejes i forhold til brugerens interesser eller grundlæggende rettigheder og frihedsrettigheder for at afgøre, hvilke af disse bør beskyttes i henhold til artikel 1, stk. 1, i direktiv 95/46[40].

103. Der bør efter min opfattelse ikke tilføjes mere for så vidt angår de betingelser, i henhold til hvilke denne afvejning skal ske i den sag, som har givet anledning til den præjudicielle forelæggelse. Bundesgerichtshof (forbundsdomstol) stiller ikke spørgsmål herom, eftersom den fokuserer på løsningen på et spørgsmål, der går forud for denne afvejning, nemlig om denne afvejning kan finde sted.

104. Det forekommer endelig overflødigt at gøre opmærksom på, at den forelæggende ret kan tage højde for eventuelle retsforskrifter, som medlemsstaterne har vedtaget inden for rammerne af den tilladelse, der er indeholdt i artikel 13, stk. 1, litra d), i direktiv 95/46, for at begrænse de forpligtelser og rettigheder, der er fastlagt i direktivets artikel 6, når dette er nødvendigt af hensyn til bl.a. »[...] forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager [...]«. Den forelæggende ret berører heller ikke dette aspekt, om end den uden tvivl er bevidst om, at begge artikler foreligger.

37 — Kapitel II: »Almindelige betingelser for lovlig behandling af personoplysninger«, som omfatter artikel 5-21 i direktiv 95/46.

38 — Dom af 24.11.2011 (C-468/10 og C-469/10, EU:C:2011:777, præmis 36).

39 — Ibidem, præmis 47.

40 — På retsmødet afviste Patrick Breyers forsvarer, at det er nødvendigt at registrere dynamiske ip-adresser for at sikre funktionsdygtigheden af internettjenesterne i tilfælde af eventuelle angreb. Jeg mener ikke, at det er muligt at give et kategorisk svar på dette problem. Løsningen herpå bør derimod findes i hver enkelt sag ved at afveje interessen hos indehaveren af webstedet i forhold til brugernes rettigheder og interesser.

105. Jeg foreslår derfor, at det andet præjudicielle spørgsmål besvares med, at artikel 7, litra f), i direktiv 95/46 skal fortolkes således, at den er til hinder for en national bestemmelse, hvis fortolkning forhindrer, at en tjenesteudbyder indsamler og behandler en brugers personoplysninger uden dennes samtykke med henblik på at sikre funktionsdygtigheden af telekommunikationstjenesten, når hvert enkelt besøg er afsluttet.

VI – Forslag til afgørelse

106. På baggrund af det ovenstående foreslår jeg Domstolen at besvare de præjudicielle spørgsmål således:

»1) I henhold til artikel 2, litra a), i Europa-Parlamentet og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger udgør en dynamisk ip-adresse, hvormed en bruger har besøgt et websted fra en udbyder af telekommunikationstjenester, en »personoplysning« for sidstnævnte, for så vidt som en internetudbyder råder over yderligere viden, som, sammenholdt med den dynamiske ip-adresse, gør det muligt at identificere brugeren.

2) Artikel 7, litra f), i direktiv 95/46 skal fortolkes således, at formålet med at sikre telekommunikationstjenestens generelle funktionsdygtighed i princippet kan betragtes som en legitim interesse, hvis opfyldelse begrunder, at disse personoplysninger anvendes, hvilket er betinget af en vurdering af, hvorvidt denne interesse har forrang for den berørte persons interesser eller grundlæggende rettigheder. En national bestemmelse, der ikke giver mulighed for at tage højde for denne legitime interesse, er ikke forenelig med nævnte artikel.«