CONCLUSIE VAN ADVOCAAT-GENERAAL
M. CAMPOS SÁNCHEZ-BORDONA
van 12 mei 2016 [1]

Zaak C-582/14

Patrick Breyer
tegen
Bundesrepublik Deutschland

[verzoek van het Bundesgerichtshof (Duitsland) om een prejudiciële beslissing]

„Verwerking van persoonsgegevens — Richtlijn 95/46/EG — Artikel 2, onder a), en artikel 7, onder f) — Begrip ‚persoonsgegevens' — IP-adressen — Bewaring door een aanbieder van elektronische mediadiensten — Nationale regeling volgens welke geen rekening kan worden gehouden met het legitieme belang van de voor de verwerking verantwoordelijke"

1. Een internetprotocoladres (hierna: IP-adres) is een binaire numerieke reeks die, toegekend aan een apparaat (een computer, tablet of smartphone), dat apparaat identificeert en het mogelijk maakt om toegang tot het elektronischecommunicatienetwerk te krijgen. Om toegang tot internet te krijgen moet het apparaat de numerieke reeks gebruiken die door de internetproviders is toegewezen. Het IP-adres wordt doorgegeven aan de server waar de te consulteren website is opgeslagen.

2. In het bijzonder wijzen de internetproviders (in het algemeen de telefoonmaatschappijen) hun klanten tijdelijk zogenoemde „dynamische IP-adressen" toe voor elke verbinding met internet en wijzigen die weer bij latere verbindingen. Dezelfde maatschappijen houden een register bij waarin staat vermeld welk IP-adres zij op welk moment aan een bepaald apparaat [2] hebben toegewezen.

3. Ook de eigenaren van de websites waar men via dynamische IP-adressen toegang toe krijgt, houden meestal bij welke pagina's zijn bezocht, het tijdstip waarop en vanaf welk dynamisch IP-adres. Deze registratie kan, technisch gezien, na afloop van de betrokken verbinding van elke gebruiker voor onbepaalde tijd worden bewaard.

4. Een dynamisch IP-adres alléén is voor de aanbieder van diensten niet voldoende om de gebruiker van zijn webpagina te identificeren. Hij kan dit echter wél wanneer hij het dynamische IP-adres combineert met aanvullende gegevens die in handen zijn van de internetprovider.

1 — Oorspronkelijke taal: Spaans.

2 — Artikel 5 van richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van richtlijn 2002/58/EG (PB 2006, L 105, blz. 54) verplichtte de lidstaten onder andere om, ten behoeve van het onderzoeken, opsporen en vervolgen van ernstige criminaliteit, „datum en tijdstip van de log-in en log-off van een internetsessie, [...] samen met het IP-adres, hetzij statisch, hetzij dynamisch, dat door de aanbieder van een internettoegangsdienst aan een communicatie is toegewezen, en de gebruikersidentificatie van de abonnee of geregistreerde gebruiker" te bewaren.

5. In deze zaak gaat het om de vraag of dynamische IP-adressen een persoonsgegeven zijn in de zin van artikel 2, onder a), van richtlijn 95/46/EG. [3] Voor het antwoord daarop moet eerst worden bepaald hoe relevant het daarvoor is dat de aanvullende gegevens die nodig zijn voor de identificatie van de gebruiker, niet in het bezit zijn van de eigenaar van de website, maar van een derde (concreet, de internetprovider).

6. Dit is een nieuwe vraag voor het Hof, want in punt 51 van het arrest Scarlet Extended [4] heeft het verklaard dat IP-adressen „beschermde persoonsgegevens" zijn, „aangezien zij de precieze identificatie van die gebruikers mogelijk maken", maar die zaak speelde zich af binnen een context waarin de verzameling en de identificatie van de IP-adressen door de internetprovider werd verricht [5] en niet door een leverancier van content, zoals in de onderhavige zaak.

7. Als de dynamische IP-adressen voor de aanbieder van diensten persoonsgegevens zijn, dan moet vervolgens worden onderzocht of de verwerking ervan binnen de werkingssfeer van richtlijn 95/46 valt.

8. Het is mogelijk dat persoonsgegevens niet onder de bescherming van richtlijn 95/46 vallen, als bijvoorbeeld het doel van de verwerking de instelling van strafvervolging tegen eventuele hackers van de website is. In die situatie is richtlijn 95/46, overeenkomstig artikel 3, lid 2, eerste streepje, niet van toepassing.

9. Voorts moet worden bepaald of de aanbieder van diensten (in deze zaak de Bondsrepubliek Duitsland) die de dynamische IP-adressen opslaat wanneer een gebruiker zijn webpagina's bezoekt, optreedt als overheid of als particulier.

10. Als richtlijn 95/46 van toepassing is, dan moet ten slotte worden bepaald in welke mate artikel 7, onder f), verenigbaar is met een nationale regeling die de reikwijdte van een van de daarin gestelde voorwaarden voor rechtvaardiging van de verwerking van persoonsgegevens beperkt.

I – **Toepasselijke bepalingen**

A – *Unierecht*

11. Overweging 26 van richtlijn 95/46 luidt als volgt:

„(26) Overwegende dat de beschermingsbeginselen moeten gelden voor elk gegeven betreffende een geïdentificeerde of identificeerbare persoon; dat, om te bepalen of een persoon identificeerbaar is, moet worden gekeken naar alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs door degene die voor de verwerking verantwoordelijk is dan wel door enig ander persoon in te zetten zijn om genoemde persoon te identificeren; dat de beschermingsbeginselen niet van toepassing zijn op gegevens die op zodanige wijze anoniem zijn gemaakt dat de persoon waarop ze betrekking hebben niet meer identificeerbaar is; dat de gedragscodes in de zin van artikel 27 een nuttig instrument kunnen zijn om een indicatie te geven omtrent de middelen waarmee de gegevens anoniem kunnen worden gemaakt en kunnen worden bewaard in een vorm die identificatie van de betrokkene niet langer mogelijk maakt".

3 — Richtlijn van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (PB 1995, L 281, blz. 31).

4 — Arrest van 24 november 2011 (C-70/10, EU:C:2011:771, punt 51).

5 — Dat is ook het geval in het arrest van 19 april 2012, Bonnier Audio e.a. (C-461/10, EU:C:2012:219, punten 51 en 52).

12. Artikel 1 van richtlijn 95/46 bepaalt het volgende:

„1. De lidstaten waarborgen in verband met de verwerking van persoonsgegevens, overeenkomstig de bepalingen van deze richtlijn, de bescherming van de fundamentele rechten en vrijheden van natuurlijke personen, inzonderheid van het recht op persoonlijke levenssfeer.

2. De lidstaten mogen het vrije verkeer van persoonsgegevens tussen lidstaten beperken noch verbieden om redenen die met de uit hoofde van lid 1 gewaarborgde bescherming verband houden."

13. Artikel 2 van richtlijn 95/46 luidt als volgt:

„Voor de toepassing van deze richtlijn wordt verstaan onder:

a) ‚persoonsgegevens' iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon, hierna ‚betrokkene' te noemen; als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer of van een of meer specifieke elementen die voor zijn fysieke, fysiologische, psychische, economische, culturele of sociale identiteit kenmerkend zijn;

b) ‚verwerking van persoonsgegevens', hierna ‚verwerking' te noemen, elke bewerking of elk geheel van bewerkingen met betrekking tot persoonsgegevens, al dan niet uitgevoerd met behulp van geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op enigerlei andere wijze ter beschikking stellen, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens;

[...]

d) ‚voor de verwerking verantwoordelijke', de natuurlijke of rechtspersoon, de overheidsinstantie, de dienst of enig ander lichaam die, respectievelijk dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer het doel van en de middelen voor de verwerking worden vastgesteld bij nationale of communautaire wettelijke of bestuursrechtelijke bepalingen, kan in het nationale of communautaire recht worden bepaald wie de voor de verwerking verantwoordelijke is of volgens welke criteria deze wordt aangewezen;

[...]

f) ‚derde', de natuurlijke of rechtspersoon, de overheidsinstantie, de dienst of enig ander lichaam, niet zijnde de betrokkene, noch de voor de verwerking verantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de voor de verwerking verantwoordelijke of de verwerker gemachtigd zijn om de gegevens te verwerken;

[...]"

14. Onder het opschrift „Werkingssfeer" bepaalt artikel 3 van richtlijn 95/46:

„1. De bepalingen van deze richtlijn zijn van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede op de niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

2. De bepalingen van deze richtlijn zijn niet van toepassing op de verwerking van persoonsgegevens:

— die met het oog op de uitoefening van niet binnen de werkingssfeer van het gemeenschapsrecht vallende activiteiten geschiedt zoals die bedoeld in de titels V en VI van het Verdrag betreffende de Europese Unie en in ieder geval verwerkingen die betrekking hebben op de openbare veiligheid, defensie, de veiligheid van de staat (waaronder de economie van de staat, wanneer deze verwerkingen in verband staan met vraagstukken van staatsveiligheid), en de activiteiten van de staat op strafrechtelijk gebied;

[...]"

15. Hoofdstuk II van richtlijn 95/46, met het opschrift „Algemene voorwaarden voor de rechtmatigheid van de verwerking van persoonsgegevens", vangt aan met artikel 5, dat bepaalt dat „de lidstaten [...] binnen de grenzen van de bepalingen van dit hoofdstuk nader de voorwaarden [bepalen] waaronder de verwerking van persoonsgegevens rechtmatig is".

16. Artikel 6 van richtlijn 95/46 luidt:

„1. De lidstaten bepalen dat de persoonsgegevens:

a) eerlijk en rechtmatig moeten worden verwerkt;

b) voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden moeten worden verkregen en vervolgens niet worden verwerkt op een wijze de onverenigbaar is met die doeleinden. Verdere verwerking van de gegevens voor historische, statistische of wetenschappelijke doeleinden wordt niet als onverenigbaar beschouwd, mits de lidstaten passende garanties bieden;

c) toereikend, ter zake dienend en niet bovenmatig moeten zijn, uitgaande van de doeleinden waarvoor zij worden verzameld of waarvoor zij vervolgens worden verwerkt;

d) nauwkeurig dienen te zijn en, zo nodig, dienen te worden bijgewerkt; alle redelijke maatregelen dienen te worden getroffen om de gegevens die, uitgaande van de doeleinden waarvoor zij worden verzameld of waarvoor zij vervolgens worden verwerkt, onnauwkeurig of onvolledig zijn, uit te wissen of te corrigeren;

e) in een vorm die het mogelijk maakt de betrokkenen te identificeren, niet langer mogen worden bewaard dan voor de verwezenlijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, noodzakelijk is. De lidstaten voorzien in passende waarborgen voor persoonsgegevens die langer dan hierboven bepaald voor historische, statistische of wetenschappelijke doeleinden worden bewaard.

2. Op de voor de verwerking verantwoordelijke rust de plicht om voor de naleving van het bepaalde in lid 1 zorg te dragen."

17. Artikel 7 van richtlijn 95/46 luidt:

„De lidstaten bepalen dat de verwerking van persoonsgegevens slechts mag geschieden indien:

a) de betrokkene daarvoor zijn ondubbelzinnige toestemming heeft verleend, of

b) de verwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene, of

c) de verwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan de voor de verwerking verantwoordelijke onderworpen is, of

d) de verwerking noodzakelijk is ter vrijwaring van een vitaal belang van de betrokkene, of

e) de verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang of die deel uitmaakt van de uitoefening van het openbaar gezag die aan de voor de verwerking verantwoordelijke of de derde aan wie de gegevens worden verstrekt, [...] is opgedragen, of

f) de verwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de voor de verwerking verantwoordelijke of van de derde(n) aan wie de gegevens worden verstrekt, mits het belang of de fundamentele rechten en vrijheden van de betrokkene die aanspraak maakt op bescherming uit hoofde van artikel 1, lid 1, van deze richtlijn, niet prevaleren."

18. Artikel 13 van richtlijn 95/46 bepaalt:

„1. De lidstaten kunnen wettelijke maatregelen treffen ter beperking van de reikwijdte van de in artikel 6, lid 1, artikel 10, artikel 11, lid 1, artikel 12 en artikel 21 bedoelde rechten en plichten indien dit noodzakelijk is ter vrijwaring van

a) de veiligheid van de staat;

b) de landsverdediging;

c) de openbare veiligheid;

d) het voorkomen, het onderzoeken, opsporen en vervolgen van strafbare feiten of schendingen van de beroepscodes voor gereglementeerde beroepen;

e) een belangrijk economisch en financieel belang van een lidstaat of van de Europese Unie, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden;

f) een taak op het gebied van controle, inspectie of regelgeving, verbonden, ook al is dit incidenteel, met de uitoefening van het openbaar gezag in de onder c), d) en e), bedoelde gevallen;

g) de bescherming van de betrokkene of van de rechten en vrijheden van anderen.

[...]"

B – *Nationaal recht*

19. § 12 van het Telemediengesetz (Duitse wet inzake elektronische media; hierna: „TMG")[6] bepaalt:

„(1) De aanbieder van diensten mag persoonsgegevens in verband met de terbeschikkingstelling van elektronische media slechts verzamelen en benutten, voor zover deze wet of een ander wettelijk voorschrift dat expliciet op elektronische media betrekking heeft, dit toestaat of de gebruiker zijn toestemming heeft gegeven.

6 — Wet van 26 februari 2007 (BGBl. 2007 I, blz. 179).

(2) De aanbieder van diensten mag persoonsgegevens die voor de terbeschikkingstelling van elektronische media zijn verzameld, slechts voor andere doeleinden benutten, voor zover deze wet of een ander wettelijk voorschrift dat expliciet op elektronische media betrekking heeft, dit toestaat of de gebruiker zijn toestemming heeft gegeven.

(3) Tenzij iets anders is bepaald, zijn de voor de bescherming van persoonsgegevens geldende regels van toepassing, ook wanneer de gegevens niet automatisch worden verwerkt."

20. § 15 TMG luidt:

„(1) De aanbieder van diensten mag persoonsgegevens van een gebruiker slechts verzamelen en benutten, voor zover dit nodig is om het gebruik van elektronische media mogelijk te maken en te factureren (gebruiksgegevens). Als gebruiksgegevens worden in het bijzonder aangemerkt:

1. criteria met het oog op de identificatie van de gebruiker;

2. gegevens over begin en einde van het betrokken gebruik, alsook over de omvang ervan, en

3. gegevens over de telecommunicatiediensten waarvan de gebruiker heeft gebruikgemaakt.

(2) De aanbieder van diensten mag gebruiksgegevens van een gebruiker over het benutten van verschillende elektronische media samenvoegen, voor zover dit voor de facturering aan de gebruiker nodig is.

[...]

(4) De aanbieder van diensten mag gebruiksgegevens na afloop van het gebruik benutten, voor zover zij voor de facturering aan de gebruiker nodig zijn (factuurgegevens). Om aan wettelijke, statutaire of contractuele bewaartermijnen te voldoen, mag de aanbieder van diensten de gegevens afschermen. [...]"

21. Overeenkomstig § 3, lid 1, van het Bundesdatenschutzgesetz (federale gegevensbeschermingswet; hierna: „BDSG")[7] zijn „persoonsgegevens [...] concrete gegevens over persoonlijke of zakelijke omstandigheden van een geïdentificeerde of identificeerbare natuurlijke persoon (de betrokkene). [...]"

II – **Feiten**

22. P. Breyer heeft tegen de Bondsrepubliek Duitsland een vordering tot staking van de bewaring van IP-adressen ingesteld.

23. Tal van federale instellingen exploiteren voor het publiek toegankelijke internetportalen waarop zij actuele informatie ter beschikking stellen. Teneinde internetaanvallen af te weren en strafvervolging van de aanvallers mogelijk te maken, wordt bij de meeste van deze portalen elke toegang in logbestanden geregistreerd. In die bestanden bewaren zij, ook na de afloop van het betrokken gebruik, de naam van het opgevraagde bestand of van de opgevraagde pagina's, de zoektermen die in de zoekvelden werden ingevoerd, het moment van opvraging, de verstuurde hoeveelheid gegevens, het bericht of de opvraging is gelukt en het IP-adres van de computer van waaraf de toegang plaatsvindt.

7 — Wet van 20 december 1990 (BGBl. 1990 I, blz. 2954).

24. Breyer, die verschillende dergelijke websites bezocht, vordert de veroordeling van de Bondsrepubliek Duitsland tot staking van het na afloop van het betrokken gebruik bewaren of door derden doen bewaren van het IP-adres van het host-systeem van waaraf de toegang plaatsvond, tenzij de bewaring in geval van storing nodig was om de beschikbaarheid van de elektronische mediadienst te herstellen.

25. De vordering van Breyer werd in eerste aanleg afgewezen. In hoger beroep werd deze echter gedeeltelijk toegewezen en werd de Bondsrepubliek Duitsland veroordeeld tot staking van het na afloop van het betrokken gebruik bewaren van het IP-adres. Aan dit bevel tot staking was de voorwaarde verbonden dat verzoeker zijn personalia tijdens het gebruik ook in de vorm van een e-mailadres opgaf en de bewaring niet nodig was om de beschikbaarheid van de elektronische mediadienst te herstellen.

III – **Prejudiciële vragen**

26. Nadat beide partijen een verzoek tot „Revision" hadden ingesteld, heeft de VIe kamer van het Bundesgerichtshof de volgende prejudiciële vragen gesteld, die op 17 december 2014 zijn ingediend:

„1) Dient artikel 2, onder a), van richtlijn 95/46/EG [...] aldus te worden uitgelegd dat een internetprotocoladres (IP-adres) dat een aanbieder van diensten opslaat wanneer zijn internetsite wordt bezocht, voor deze aanbieder reeds dan een persoonsgegeven vormt, wanneer een derde (in casu: de internetprovider) beschikt over de aanvullende gegevens die nodig zijn om de betrokken persoon te identificeren?

2) Verzet artikel 7, onder f), van de richtlijn betreffende gegevensbescherming zich tegen een regel van nationaal recht op grond waarvan de aanbieder van diensten persoonsgegevens van een gebruiker zonder diens toestemming enkel mag verzamelen en benutten voor zover dit nodig is om het concrete gebruik van de elektronische mediadienst door de betrokken gebruiker mogelijk te maken en te factureren en op grond waarvan de doelstelling, die erin bestaat de goede werking van de elektronische mediadienst in het algemeen te waarborgen, niet rechtvaardigt dat de gegevens worden benut na afloop van het betrokken gebruik?"

27. De verwijzende rechter zet uiteen dat verzoeker overeenkomstig het Duitse recht een vordering tot staking van de opslag van de IP-adressen kan indienen, als die opslag overeenkomstig het recht inzake gegevensbescherming een ongeoorloofde inbreuk op verzoekers algemene persoonsrecht – meer specifiek het recht op „informatieve zelfbeschikking" – vormt [§§ 1004, lid 1, en 823, lid 1, van het Bürgerliches Gesetzbuch (Duits burgerlijk wetboek) juncto de artikelen 1 en 2 van het Grundgesetz (Duitse federale grondwet)].

28. Dat zou zo zijn als a) het IP-adres – in elk geval in combinatie met het tijdstip van de toegang tot een website – behoort tot de „persoonsgegevens" in de zin van artikel 2, onder a), juncto overweging 26, tweede deeloverweging, van richtlijn 95/46, respectievelijk § 12, leden 1 en 3, TMG juncto § 3, lid 1, BDSG, en b) er geen sprake is van een rechtvaardigingsgrond in de zin van artikel 7, onder f), van richtlijn 95/46, respectievelijk § 12, leden 1 en 3, en § 15, leden 1 en 4, TMG.

29. Volgens het Bundesgerichtshof is het voor de uitlegging van het nationale recht (§ 12, lid 1, TMG) noodzakelijk te weten hoe het persoonlijke karakter van de gegevens waar artikel 2, onder a), van richtlijn 95/46 betrekking op heeft, moet worden begrepen.

30. Daarnaast wijst de verwijzende rechter erop dat, aangezien overeenkomstig § 15, lid 1, TMG, de aanbieder van diensten de persoonsgegevens van een gebruiker enkel kan verzamelen en benutten voor zover dit nodig is om het gebruik van elektronische mediadiensten mogelijk te maken en te factureren (gebruiksgegevens) [8], de uitlegging van die bepaling nauw verbonden is met die van artikel 7, onder f), van richtlijn 95/46.

IV – **Procedure bij het Hof en argumenten van partijen**

31. Schriftelijke opmerkingen zijn ingediend door de Duitse, de Oostenrijkse en de Portugese regering en de Commissie. Enkel de Commissie en Breyer zijn op de zitting van 25 februari 2016 verschenen. De Duitse regering heeft besloten niet te verschijnen.

A – *Argumenten van partijen inzake de eerste vraag*

32. Breyer stelt dat ook gegevens die uitsluitend theoretisch – namelijk uitgaande van een abstract risico van identificatie – te combineren zijn, persoonsgegevens zijn, en dat het daarbij van weinig belang is of die combinatie in praktijk wordt gebracht. Naar zijn mening betekent het feit dat een instantie relatief gezien niet in staat is een persoon te identificeren door gebruik te maken van het IP-adres, niet, dat er voor die persoon geen risico aanwezig is. Verder is volgens hem relevant dat Duitsland zijn IP-gegevens bewaart om, als dat nodig is, eventuele aanvallen te herkennen en strafvervolging tegen de aanvallers in te stellen, hetgeen wordt toegestaan bij § 113 van het Telekommunikationsgesetz en bij tal van gelegenheden is gebeurd.

33. De Duitse regering meent dat de eerste vraag ontkennend dient te worden beantwoord, omdat dynamische IP-adressen de persoon niet „geïdentificeerd" maken in de zin van artikel 2, onder a), van richtlijn 95/46. Om te uit te maken of zij de persoon „identificeerbaar" maken in de zin van dezelfde bepaling, moet het onderzoek naar de *identificeerbaarheid* geschieden via de „relatieve" benadering. Naar haar mening is dat af te leiden uit overweging 26 van richtlijn 95/46, volgens welke alleen moet worden gekeken naar de middelen waarvan mag worden aangenomen dat zij „redelijkerwijs" door degene die voor de verwerking verantwoordelijk is, dan wel door enig ander persoon, in te zetten zijn om genoemde persoon te identificeren. Die specificatie zou erop wijzen dat de Uniewetgever situaties waarin het voor een willekeurige derde objectief gezien mogelijk is de persoon te identificeren, niet binnen de werkingssfeer van richtlijn 95/46 heeft willen laten vallen.

34. Ook meent de Duitse regering dat het begrip „persoonsgegevens" in de zin van artikel 2, onder a), van richtlijn 95/46 dient te worden uitgelegd tegen de achtergrond van het doel van deze richtlijn, namelijk de eerbiediging van de grondrechten waarborgen. De noodzaak natuurlijke personen te beschermen kan op verschillende manieren worden bekeken naargelang van de vraag wie de gegevens bezit en of diegene al dan niet beschikt over de middelen om zich van die gegevens te bedienen teneinde de personen te identificeren.

35. De Duitse regering is van mening dat Breyer niet identificeerbaar is op basis van een combinatie van de IP-adressen met andere gegevens die door de leveranciers van content worden bewaard. Daarvoor zou informatie moeten worden gebruikt die in handen is van de internetproviders, die deze informatie niet zonder wettelijke basis aan de aanbieders van content mogen doorgeven.

8 — Gebruiksgegevens zijn volgens het Bundesgerichtshof gegevens die de gebruiker identificeren, over het begin en het einde van de opvraging, de hoeveelheid verstuurde gegevens en de elektronische mediadiensten die door hem zijn gebruikt.

36. De Oostenrijkse regering meent daarentegen dat het antwoord op de vraag bevestigend moet zijn. Overeenkomstig overweging 26 van richtlijn 95/46 is het, om een persoon als identificeerbaar te beschouwen, niet nodig dat alle gegevens waarmee hij geïdentificeerd kan worden in handen zijn van één instantie. Zo kan een IP-adres een persoonsgegeven zijn indien een derde (bijvoorbeeld de internetprovider) over de middelen beschikt waarmee hij de eigenaar van dat IP-adres zonder al te veel moeite kan identificeren.

37. Ook de Portugese regering neigt naar een bevestigend antwoord en stelt dat het IP-adres, in combinatie met de datum van de zoekactie, een persoonsgegeven vormt voor zover deze combinatie kan leiden tot identificatie van de gebruiker door een andere instantie dan die welke het IP-adres heeft opgeslagen.

38. De Commissie stelt eveneens voor om de vraag bevestigend te beantwoorden en baseert zich daarbij op de uitspraak van het Hof in de zaak Scarlet Extended[9]. De Commissie stelt dat, aangezien het doel van de opslag van IP-adressen juist is om bij internetaanvallen de gebruikers te identificeren, het gebruik van de aanvullende gegevens die door de internetproviders worden opgeslagen een middel is dat in de zin van overweging 26 van richtlijn 95/46 „redelijkerwijs" kan worden ingezet. Naar de mening van de Commissie pleiten zowel het doel van de richtlijn als de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie (hierna: „Handvest") voor een ruime uitlegging van artikel 2, onder a), van richtlijn 95/46.

B – *Argumenten van partijen inzake de tweede vraag*

39. Breyer meent dat artikel 7, onder f), van richtlijn 95/46 een algemene bepaling is die concretisering behoeft om in praktijk te worden gebracht. Volgens de rechtspraak van het Hof zou het er dus om gaan, de omstandigheden van de concrete zaak af te wegen en te bepalen of er groepen zijn met een gerechtvaardigd belang in de zin van die bepaling, en is het niet alleen toegestaan maar zelfs noodzakelijk dat er specifieke bepalingen voor die groepen worden vastgesteld voor de toepassing van dat artikel. In die situatie zou volgens Breyer de nationale regeling verenigbaar zijn met artikel 7, onder f), van richtlijn 95/46, aangezien het openbare internetportaal geen belang heeft bij de opslag van persoonsgegevens, of omdat het belang van de bescherming van de anonimiteit zwaarder weegt. Naar zijn opvatting is echter een systematische en gepersonaliseerde opslag van de gegevens niet in overeenstemming met een democratische maatschappij, noch noodzakelijk of proportioneel ter waarborging van de goede werking van de elektronische communicatiemiddelen, die ook prima kan worden gewaarborgd zonder de opslag van persoonsgegevens, zoals websites van sommige federale ministeries zouden bewijzen.

40. De Duitse regering stelt dat het niet nodig is de tweede vraag te beantwoorden, omdat die enkel is gesteld voor het geval dat de eerste vraag bevestigend zou moeten worden beantwoord, hetgeen naar haar mening, om de bovengenoemde redenen, niet het geval is.

41. De Oostenrijkse regering stelt voor om te antwoorden dat richtlijn 95/46 zich in algemene zin niet verzet tegen de opslag van gegevens als die welke in het hoofdgeding aan de orde zijn, wanneer die opslag noodzakelijk is voor de waarborging van de goede werking van de elektronische communicatiemiddelen. Naar de mening van deze regering kan een beperkte opslag van het IP-adres, nadat de opvraging van een webpagina is beëindigd, rechtmatig zijn gelet op de verplichting van de voor de verwerking van de persoonsgegevens verantwoordelijke om de maatregelen ter bescherming van die gegevens ten uitvoer te leggen die in artikel 17, lid 1, van richtlijn 95/46 worden verlangd. De strijd tegen internetaanvallen kan rechtvaardigen dat gegevens inzake vorige aanvallen worden onderzocht en dat aan sommige IP-adressen de toegang tot die internetpagina wordt ontzegd. De

9 — Arrest van 24 november 2011 (C-70/10, EU:C:2011:771, punt 51).

vraag of het uit het perspectief van het doel, de goede werking van het elektronische communicatiemiddel te waarborgen, evenredig is om gegevens op te slaan als die welke in het hoofdgeding aan de orde zijn, dient per geval te worden onderzocht, rekening houdend met de beginselen van artikel 6, lid 1, van richtlijn 95/46.

42. De Portugese regering houdt staande dat artikel 7, onder f), van richtlijn 95/46 zich niet verzet tegen de in het hoofdgeding aan de orde zijnde nationale bepalingen, omdat de Duitse wetgever de in die bepaling verlangde afweging al zou hebben verricht tussen enerzijds het gerechtvaardigde belang van de voor de verwerking van persoonsgegevens verantwoordelijke, en anderzijds de rechten en vrijheden van de betrokkenen.

43. De Commissie is van mening dat de nationale regeling waarin artikel 7, onder f), van richtlijn 95/46 is omgezet, de doelstellingen van de verwerking van persoonsgegevens zodanig moet definiëren dat zij voor het betrokken individu voorzienbaar zijn. Zij meent dat de Duitse regeling niet aan die eis voldoet, omdat § 15, lid 1, TMG bepaalt dat de opslag van IP-adressen is toegestaan „wanneer dat nodig is om het gebruik [...] van elektronische mediadiensten mogelijk te maken".

44. De Commissie stelt dus voor om op de tweede vraag te antwoorden dat artikel 7, onder f), zich verzet tegen de uitlegging van een nationale bepaling volgens welke een overheidsorgaan dat als aanbieder van diensten optreedt, persoonsgegevens van een gebruiker zonder diens toestemming kan verzamelen en benutten, ook al is het doel daarvan de goede werking van het elektronische communicatiemiddel in het algemeen te waarborgen, als de betrokken nationale bepaling dat doel niet op een voldoende duidelijke en precieze manier vaststelt.

V – **Beoordeling**

A – *Eerste vraag*

1. Afbakening van de vraag

45. Volgens de bewoordingen waarin het Bundesgerichtshof zijn eerste vraag heeft geformuleerd, wenst het daarmee te vernemen of een IP-adres waarmee toegang tot een website wordt verkregen, voor het overheidsorgaan dat eigenaar is van deze website reeds dan een persoonsgegeven [in de zin van artikel 2, onder a), van richtlijn 95/46] vormt, wanneer de internetprovider beschikt over aanvullende gegevens die de identificatie van de betrokkene mogelijk maken.

46. Aldus geformuleerd is de vraag duidelijk genoeg om andere vragen die in abstracto over de juridische aard van IP-adressen binnen de context van de bescherming van persoonsgegevens zouden kunnen worden gesteld, meteen uit te sluiten.

47. In de eerste plaats doelt het Bundesgerichtshof uitsluitend op „dynamische IP-adressen", namelijk adressen die tijdelijk bij elke internetverbinding worden toegewezen en die bij latere verbindingen worden gewijzigd. „Vaste of statische IP-adressen", die gekenmerkt worden door hun onveranderlijkheid en door het feit dat zij de identificatie van het apparaat dat met internet is verbonden voortdurend mogelijk maken, blijven dus buiten beschouwing.

48. In de tweede plaats gaat de verwijzende rechter uit van de veronderstelling dat, in het hoofdgeding, de eigenaar van de website niet in staat is om via het dynamische IP-adres degenen die zijn website bezoeken te identificeren, en dat die eigenaar zelf niet beschikt over aanvullende gegevens die, in combinatie met dat IP-adres, de identificatie van de bezoeker mogelijk maken. Het Bundesgerichtshof lijkt van oordeel te zijn dat in deze context het dynamische IP-adres *voor de eigenaar van de website* geen persoonsgegeven in de zin van artikel 2, onder a), van richtlijn 95/46 is.

49. De twijfel van de verwijzende rechter heeft te maken met de mogelijkheid dat het dynamische IP-adres voor de eigenaar van de website kan worden aangemerkt als een persoonsgegeven *indien een derde beschikt over aanvullende gegevens* die het mogelijk maken om, in combinatie met het IP-adres, de bezoekers van hun website te identificeren. Echter – en dit is nog een belangrijke precisering – het Bundesgerichtshof spreekt niet over een willekeurige derde die over de aanvullende gegevens beschikt, maar uitsluitend over de internetprovider (de verwijzende rechter sluit dus andere mogelijke bezitters van dit soort gegevens uit).

50. Onder meer de volgende vragen blijven dus buiten de discussie: a) Zijn statische IP-adressen persoonsgegevens in de zin van richtlijn 95/46?[10] b) Zijn dynamische IP-adressen altijd en onder alle omstandigheden persoonsgegevens in de zin van die richtlijn? c) Moeten, ten slotte, dynamische IP-adressen noodzakelijkerwijs als persoonsgegevens worden aangemerkt zodra er sprake is van een willekeurige derde die in staat is om die adressen te gebruiken voor de identificatie van de internetgebruikers?

51. Het Hof moet dus enkel bepalen of een dynamisch IP-adres voor de aanbieder van een internetdienst een persoonsgegeven is, wanneer de telefoonmaatschappij die de toegang tot internet aanbiedt (de internetprovider) aanvullende gegevens bezit die in combinatie met het IP-adres de identificatie mogelijk maken van degene die de website van de aanbieder van de internetdienst bezoekt.

2. Beantwoording van de vraag

52. De vraag van de verwijzende rechter is in de Duitse rechtswetenschap en rechtspraak al langer het voorwerp van heftige discussie tussen twee tegenovergestelde stromingen.[11] De ene stroming (die kiest voor een „objectief" of „absoluut" criterium) meent dat een gebruiker identificeerbaar is – en dat daarom het IP-adres een persoonsgegeven is dat beschermd dient te worden – wanneer hij, onafhankelijk van de mogelijkheden en middelen van de aanbieder van de internetdienst, al geïdentificeerd kan worden door de combinatie van dat dynamische IP-adres met de gegevens die een derde (bijvoorbeeld de internetprovider) heeft verschaft.

53. De andere stroming (die kiest voor een „relatief" criterium) meent dat het feit dat de uiteindelijke identificatie van de gebruiker met behulp van een derde kan worden gerealiseerd, niet voldoende is om het dynamische IP-adres als een persoonsgegeven te beschouwen. Waar het om gaat is of degene die toegang tot het gegeven heeft, in staat is om daarvan, met behulp van zijn eigen middelen, gebruik te maken en op die wijze een persoon te identificeren.

54. Wat ook de bewoordingen zijn waarin deze tegenstelling in het nationale recht wordt uitgedrukt, het antwoord van het Hof moet beperkt zijn tot de uitlegging van de twee bepalingen van richtlijn 95/46 die zowel door de verwijzende rechter als door de procespartijen zijn genoemd, namelijk artikel 2, onder a)[12], en overweging 26[13].

10 — Die vraag is door het Hof beantwoord in de arresten van 24 november 2011, Scarlet Extended (C-70/10, EU:C:2011:771, punt 51), en 19 april 2012, Bonnier Audio e.a. (C-461/10, EU:C:2012:219). In de punten 51 en 52 van dat laatste arrest heeft het Hof bepaald dat de mededeling „met het oog op identificatie, van de naam en het adres [...] van een internetgebruiker die gebruikmaakt van het IP-adres via hetwelk bestanden met beschermde werken vermoedelijk onrechtmatig zijn uitgewisseld [...] een verwerking van persoonsgegevens [vormt] in de zin van artikel 2, eerste alinea, van richtlijn 2002/58, gelezen in samenhang met artikel 2, onder b), van richtlijn 95/46".

11 — Zie over beide stromingen bijvoorbeeld Schreibauer, M., in: *Kommentar zum Bundesdatenschutzgesetz. Nebengesetze*, Esser, M., Kramer, P., en von Lewinski, K. (red.), Carl Heymanns Verlag/Wolters Kluwer, Keulen, 2014, 4e druk, § 11 Telemediengesetz (4-10); Nink, J., en Pohle, J., „Die Bestimmbarkeit des Personenbezugs. Von der IP-Adresse zum Anwendungsbereich der Datenschutzgesetze", in: *Multimedia und Recht*, 9/2015, blz. 563-567; Heidrich, J., en Wegener, C., „Rechtliche und technische Anforderungen an die Protokollierung von IT-Daten. Problemfall Logging", in: *Multimedia und Recht*, 8/2015, blz. 487-492; Leisterer, H., „Die neuen Pflichten zur Netz- und Informationssicherheit und die Verarbeitung personenbezogener Daten zur Gefahrenabwehr", in: *Computer und Recht*, 10/2015, blz. 665-670.

12 — Zie punt 13.

13 — Zie punt 11.

55. Enkel al doordat de dynamische IP-adressen informatie verschaffen over de datum en het tijdstip van de toegang tot een website vanaf een computer (of een ander apparaat), leggen zij bepaalde gedragspatronen van de internetgebruikers bloot en betekenen zij dus een mogelijke inbreuk op het recht op eerbiediging van hun privéleven [14] dat gewaarborgd wordt door artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden en door artikel 7 van het Handvest. Tegen de achtergrond van die bepalingen alsook tegen die van artikel 8 van het Handvest moet richtlijn 95/46 [15] worden uitgelegd. De partijen in de procedure trekken deze premisse niet in twijfel. Als zodanig maakt zij geen deel uit van de prejudiciële vraag.

56. De persoon op wie deze details betrekking hebben is geen „geïdentificeerde natuurlijke persoon". De datum en het tijdstip van een verbinding of het nummer voor de toegang tot de website onthullen niet rechtstreeks en onmiddellijk wie de natuurlijke persoon is die eigenaar is van het apparaat waarmee de website wordt bezocht, en evenmin de identiteit van degene die dat apparaat gebruikt (dat kan elke willekeurige natuurlijke persoon zijn).

57. Aangezien echter een dynamisch IP-adres helpt te bepalen – hetzij alleen, hetzij in combinatie met andere gegevens – wie de eigenaar is van het voor het bezoeken van de website gebruikte apparaat, kan het worden beschouwd als informatie over een „identificeerbare persoon". [16]

58. Naar het oordeel van het Bundesgerichtshof is het dynamische IP-adres op zich onvoldoende om de gebruiker te identificeren die via dat adres op een website is gekomen. Als daarentegen de aanbieder van de internetdienst, via het dynamische IP-adres, de gebruiker zou kunnen identificeren, dan zou dat IP-adres ongetwijfeld een persoonsgegeven in de zin van richtlijn 95/46 zijn. Daar lijkt het echter niet om te gaan in de prejudiciële vraag, die ervan uitgaat dat de bij het hoofdgeding betrokken aanbieders van internetdiensten de gebruiker niet kunnen identificeren aan de hand van zijn dynamische IP-adres alléén.

59. Samen met andere gegevens maakt het dynamische IP-adres de „indirecte" identificatie van de gebruiker mogelijk – daar zijn allen het over eens. Maar rechtvaardigt de mogelijkheid dat er aanvullende gegevens bestaan die aan het dynamische IP-adres gekoppeld kunnen worden, zonder meer dat dit laatste als een persoonsgegeven in de zin van de richtlijn wordt aangemerkt? Het Hof moet beoordelen of de enkele abstracte mogelijkheid om die gegevens te achterhalen daarvoor voldoende is, of dat die gegevens daarentegen beschikbaar moeten zijn voor degene die het dynamische IP-adres al kent, of voor een derde.

60. De partijen hebben hun opmerkingen geconcentreerd op de uitlegging van overweging 26 van richtlijn 95/46, en met name van de uitdrukking „middelen waarvan mag worden aangenomen dat zij redelijkerwijs door degene die voor de verwerking verantwoordelijk is dan wel door enig ander persoon in te zetten zijn om genoemde persoon te identificeren". De vraag van de verwijzende rechter

14 — Aldus stelt advocaat-generaal Cruz Villalón in zijn conclusie in de zaak Scarlet Extended (C-70/10, EU:C:2011:255, punt 76), en zo meent ook de Europese Toezichthouder voor gegevensbescherming in zijn advies van 22 februari 2010 betreffende de huidige onderhandelingen van de Europese Unie over een Handelsovereenkomst ter bestrijding van namaak (ACTA) (PB 2010, C 147, blz. 1, punt 24), en in zijn advies van 10 mei 2010 over een voorstel voor een richtlijn van het Europees Parlement en de Raad ter bestrijding van seksueel misbruik, seksuele uitbuiting van kinderen en kinderpornografie, en tot intrekking van kaderbesluit 2004/68/JBZ (PB 2010, C 323, blz. 6, punt 11).

15 — Zie in dezelfde zin het arrest van 20 mei 2003, Österreichischer Rundfunk (C-465/00, C-138/01 en C-139/01, EU:C:2003:294, punt 68), en de conclusie van advocaat-generaal Kokott in de zaak Promusicae (C-275/06, EU:C:2007:454, punten 51 e.v.).

16 — Aangenomen mag worden dat deze persoon, tenzij het tegendeel wordt bewezen, degene is die op internet heeft rondgekeken en de betrokken site heeft bezocht. Maar ook zonder die laatste aanname zou de informatie over datum, tijdstip en het nummer voor de toegang tot een website het mogelijk maken deze toegang te koppelen aan de eigenaar van het apparaat en indirect in verband te brengen met zijn gedragslijn op het internet. Een denkbare uitzondering zouden IP-adressen vormen die zijn toegewezen aan computers in bijvoorbeeld internetcafés, waar de anonieme gebruikers onidentificeerbaar zijn en het internetverkeer in dat café geen relevante persoonlijke informatie oplevert over de eigenaren van die computers. Dit is overigens de enige uitzondering op het beginsel dat IP-adressen persoonsgegevens zijn die wordt aanvaard door de krachtens artikel 29 van richtlijn 95/46 opgerichte Groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens (de zogeheten „Groep gegevensbescherming artikel 29"). Advies 4/2007 van deze groep van 20 juni 2007 over het begrip persoonsgegevens, WP 136, is te lezen op http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

heeft geen betrekking op aanvullende gegevens die in bezit zijn van de aanbieders van internetdiensten die partij zijn in het hoofdgeding. Ook spreekt de verwijzende rechter niet over een willekeurige derde die in het bezit zou zijn van die aanvullende gegevens (die samen met het dynamische IP-adres de identificatie van de gebruiker mogelijk zouden maken), maar over de internetprovider.

61. Daarom hoeft het Hof in deze zaak dus niet alle middelen die de gedaagde in het hoofdgeding „redelijkerwijs" zou kunnen inzetten, te onderzoeken om de dynamische IP-adressen waar de gedaagde over beschikt als persoonsgegevens te kunnen kwalificeren. Aangezien het Bundesgerichtshof uitsluitend spreekt over aanvullende gegevens in handen van een derde, kan daaruit worden opgemaakt: a) hetzij dat de gedaagde zelf geen aanvullende gegevens heeft die geschikt zijn om de gebruiker te identificeren, b) hetzij dat hij, als hij wel over die gegevens beschikt, niet in staat is om – in zijn hoedanigheid van de voor de verwerking verantwoordelijke – deze gegevens „redelijkerwijs" met dat doel in te zetten, overeenkomstig overweging 26 van richtlijn 95/46.

62. Beide hypothesen hangen af van een feitelijke constatering die alleen de verwijzende rechter kan verrichten. Het Hof zou hem algemene criteria kunnen leveren voor de uitlegging van de termen „middelen waarvan mag worden aangenomen dat zij redelijkerwijs door degene die voor de verwerking verantwoordelijk is [...] in te zetten zijn", als het Bundesgerichtshof zou twijfelen aan de capaciteit van de gedaagde om „redelijkerwijs" van eigen aanvullende gegevens gebruik te maken. Aangezien dat niet het geval is, is het naar mijn mening misplaatst als het Hof nu uitleggingscriteria zou aanreiken die voor de verwijzende rechter onnodig zijn en waar hij niet om heeft gevraagd.

63. De kern van de vraag is dus of het, om de dynamische IP-adressen als persoonsgegevens te kwalificeren, van belang is dat een heel specifieke derde – de internetprovider – over aanvullende gegevens beschikt die het in combinatie met die IP-adressen mogelijk maken de gebruiker te identificeren die een bepaalde website heeft bezocht.

64. Ook hier moet overweging 26 van richtlijn 95/46 weer worden vermeld. De bewoordingen „middelen waarvan mag worden aangenomen dat zij redelijkerwijs [...] *door enig ander persoon*[17] in te zetten zijn" zouden aanleiding kunnen geven tot een uitlegging volgens welke het voldoende is dat een willekeurige derde in het bezit kan komen van aanvullende gegevens (die aan een dynamisch IP-adres kunnen worden gekoppeld om een persoon te identificeren), om dat adres op zich als een persoonsgegeven te beschouwen.

65. Deze zeer ruime uitlegging zou er in de praktijk toe leiden dat elke soort informatie als een persoonsgegeven wordt aangemerkt, ook al is die op zichzelf onvoldoende om de identificatie van een gebruiker mogelijk te maken. De mogelijkheid dat er een derde is die aanvullende gegevens bezit die met die informatie kunnen worden gecombineerd en daarom geschikt zijn om de identiteit van een persoon te onthullen, kan nooit met absolute zekerheid worden uitgesloten.

66. Naar mijn mening rechtvaardigt de mogelijkheid dat de ontwikkeling van de techniek, in een meer of minder nabije toekomst, de weg vrijmaakt voor steeds verfijndere instrumenten om informatie te verkrijgen en te verwerken, de waarborgen waarmee de persoonlijke levenssfeer op voorhand wordt omringd. De Uniewetgever heeft er bij het vastleggen van de relevante rechtscategorieën op het gebied van gegevensbescherming voor gezorgd dat daaronder gedragingen vallen die voldoende ruim en flexibel zijn geformuleerd om elke denkbare situatie te dekken.[18]

17 — Cursivering van mij.

18 — Deze doelstelling van voorzorg en preventie ligt ten grondslag aan het standpunt van de Groep gegevensbescherming artikel 29, die, zoals ik al heb aangegeven, meent dat moet worden uitgegaan van het beginsel dat IP-adressen een persoonsgegeven zijn, en die als de enige uitzondering daarop accepteert dat de aanbieder van de dienst met absolute zekerheid kan bepalen dat het adressen zijn die zijn toegewezen aan niet te identificeren personen, zoals de gebruikers in een internetcafé. Zie het slot van voetnoot 16.

67. Ik ben echter van mening dat deze bezorgdheid – die trouwens heel legitiem is – er niet toe mag leiden dat de bewoordingen worden genegeerd waarin de wetgever zijn wil heeft uitgedrukt, en dat de systematische uitlegging van overweging 26 van richtlijn 95/46 zich moet beperken tot „de middelen waarvan mag worden aangenomen dat zij redelijkerwijs in te zetten zijn" *door bepaalde derden*.

68. Net zoals overweging 26 niet doelt op elk middel dat door de voor de verwerking verantwoordelijke (in deze zaak de aanbieder van internetdiensten) in te zetten is, maar enkel op de middelen die deze „redelijkerwijs" zou kunnen inzetten, zo ook moet worden begrepen dat de wetgever met „derden" enkel diegenen bedoelt van wie, *eveneens redelijkerwijs*, mag worden aangenomen dat zij degenen zijn tot wie de voor de verwerking verantwoordelijke zich voor aanvullende gegevens voor de identificatie zal wenden. Dat zal niet gebeuren wanneer het contact met die derden in mankracht en in financiële zin feitelijk heel kostbaar, of praktisch ondoenlijk, of bij de wet verboden is. Anders zou het, zoals ik al eerder opmerkte, praktisch onmogelijk zijn om een onderscheid te maken tussen de verschillende middelen, want altijd is het denkbaar dat er een derde bestaat die – hoe onbenaderbaar hij ook voor de aanbieder van internetdiensten is – nu of in de toekomst kan beschikken over aanvullende gegevens die kunnen bijdragen tot de identificatie van een gebruiker.

69. Zoals ik al heb opgemerkt, is de derde waar het Bundesgerichtshof op doelt, een internetprovider. Het is beslist het meest redelijk om aan deze derde te denken als degene tot wie de aanbieder van de internetdiensten zich zal wenden om de benodigde aanvullende gegevens te vergaren, wanneer hij de gebruiker die via het dynamische IP-adres op zijn website is gekomen, op de meest doeltreffende, praktische en rechtstreekse manier wil identificeren. Het is geenszins een hypothetische, onbekende en ontoegankelijke derde, maar een hoofdrolspeler op internet, van wie met zekerheid bekend is dat hij in het bezit is van de gegevens die de aanbieder van de diensten nodig heeft om een gebruiker te identificeren. Zoals de verwijzende rechter opmerkt, heeft de gedaagde in het hoofdgeding inderdaad de bedoeling om zich tot deze concrete derde te wenden om de aanvullende gegevens op te vragen die hij nodig heeft.

70. De internetprovider is typisch de in overweging 26 van richtlijn 95/46 genoemde derde waarvan het meest „redelijk" kan worden aangenomen dat de aanbieder van de internetdiensten uit het hoofdgeding zich tot hem zal wenden. Het moet echter nog worden onderzocht of het verkrijgen van de aanvullende gegevens uit handen van deze derde als „redelijkerwijs" uitvoerbaar of doenlijk kan worden gekwalificeerd.

71. De Duitse regering meent dat de internetprovider, aangezien hij beschikt over een persoonsgegeven, dat gegeven niet zo maar mag vrijgeven, maar dat hij dat moet doen overeenkomstig de wettelijke bepalingen voor de verwerking van die gegevens.[19]

72. Dat is ongetwijfeld waar, want om deze informatie te mogen gebruiken moet men zich houden aan de wettelijke regeling inzake persoonsgegevens. Informatie kan enkel „op een redelijke wijze" worden verkregen, als voldaan wordt aan de voorwaarden die de toegang tot dat soort gegevens regelen, waarvan de eerste is dat het wettelijk mogelijk moet zijn die gegevens te bewaren en aan anderen door te geven. Het is juist dat de internetprovider mag weigeren de opgevraagde gegevens te verstrekken, maar het omgekeerde kan ook het geval zijn. De volstrekt „redelijke" mogelijkheid als zodanig dat gegevens worden doorgegeven, verandert het dynamische IP-adres, conform de bewoordingen van overweging 26 van richtlijn 95/46, in een persoonsgegeven voor de aanbieder van de internetdiensten.

19 — Punten 40 en 45 van haar schriftelijke opmerkingen.

73. Het gaat om een reële mogelijkheid *in het kader van de wet* en daarom om een „redelijke" mogelijkheid. De redelijke middelen van toegang tot informatie waar richtlijn 95/46 op doelt, moeten per definitie rechtmatige middelen zijn.[20] Dat is de premisse waarvan de verwijzende rechter vanzelfsprekend uitgaat, zoals de Duitse regering uiteenzet.[21] Aldus worden de juridisch relevante toegangswegen aanzienlijk beperkt, want het mogen uitsluitend rechtmatige wegen zijn. Maar zolang dergelijke toegangswegen bestaan – hoe beperkt die in de praktijk ook kunnen zijn – vormen zij een „redelijk middel" in de zin van richtlijn 95/46.

74. Daarom ben ik van mening dat de eerste vraag van het Bundesgerichtshof, in de bewoordingen waarin zij is geformuleerd, bevestigend moet worden beantwoord. Voor de aanbieder van internetdiensten moet het dynamische IP-adres worden gekwalificeerd als een persoonsgegeven, omdat er een derde (de internetprovider) is van wie redelijkerwijs kan worden aangenomen dat de aanbieder van de internetdiensten zich tot hem zal wenden om aanvullende gegevens te verkrijgen die het, in combinatie met het IP-adres, mogelijk maken om een gebruiker te identificeren.

75. De tegenovergestelde oplossing leidt tot een resultaat dat, naar mijn mening, voor mijn zienswijze pleit. Als de dynamische IP-adressen voor de aanbieder van internetdiensten geen persoonsgegeven zouden zijn, dan zou hij ze voor onbepaalde tijd kunnen bewaren en zou hij de internetprovider te allen tijde om aanvullende gegevens kunnen vragen, om die met het IP-adres te combineren en zo de gebruiker te identificeren. Onder die omstandigheden, zo erkent de Duitse regering[22], zou het dynamische IP-adres een persoonsgegeven worden, wanneer hij zonder inbreuk te maken op de regels inzake gegevensbescherming aanvullende gegevens heeft verkregen waarmee de gebruiker kan worden geïdentificeerd.

76. Het gaat dan echter om een gegeven waarvan de bewaring alleen mogelijk is geweest omdat het tot dan toe voor de aanbieder van internetdiensten niet als een persoonsgegeven is beschouwd. De juridische kwalificatie van het dynamische IP-adres als een persoonsgegeven zou aldus in handen zijn van de aanbieder van die diensten, afhankelijk van de vraag of hij op een later moment besluit dat adres te gebruiken om, in combinatie met de aanvullende gegevens die hij van een derde moet opvragen, de gebruiker te identificeren. Naar mijn mening is het overeenkomstig richtlijn 95/46 echter doorslaggevend of er een – redelijke – mogelijkheid bestaat dat er een „benaderbare" derde is die over de middelen beschikt die noodzakelijk zijn om een persoon te identificeren, en niet, dat die mogelijkheid om een beroep op deze derde te doen wordt verwezenlijkt.

77. Men zou zelfs het standpunt kunnen innemen, zoals de Duitse regering doet, dat het dynamische IP-adres pas verandert in een persoonsgegeven op het moment dat de internetprovider het ontvangt. Dan zou echter moeten worden aanvaard dat deze kwalificatie, met betrekking tot de termijn voor bewaring van het IP-adres, met terugwerkende kracht plaatsvindt en zou dat adres bijgevolg als onbestaand moeten worden beschouwd wanneer de termijn is verstreken gedurende welke het adres had kunnen worden bewaard indien het vanaf het begin als een persoonsgegeven was gekwalificeerd. Dat leidt echter tot een resultaat dat in strijd is met de geest van de wettelijke bepalingen ter bescherming van persoonsgegevens. Het argument voor een slechts tijdelijke bewaring van deze gegevens zou worden ondergraven als het belang van een kenmerk dat van het begin af inherent is aan die gegevens, namelijk hun betekenis als middel tot identificatie – op zich, of samen met andere gegevens – van een natuurlijke persoon, mogelijkerwijs eerst later wordt erkend. Ook om deze zuiver praktische reden is het redelijker om het adres reeds vanaf het begin dit karakter van persoonsgegeven toe te kennen.

20 — Het is in deze context niet van belang dat de toegang tot het persoonsgegeven de facto mogelijk is door inbreuk op de gegevensbeschermingswetten te plegen.

21 — Punten 47 en 48 van haar schriftelijke opmerkingen.

22 — Punt 36 van haar schriftelijke opmerkingen.

78. Daarom luidt mijn eerste conclusie dat artikel 2, onder a), van richtlijn 95/46 aldus moet worden uitgelegd dat een IP-adres dat een aanbieder van diensten in verband met de toegang tot zijn internetsite opslaat, voor deze aanbieder een persoonsgegeven vormt, voor zover een internetprovider beschikt over de aanvullende gegevens die nodig zijn om de betrokken persoon te identificeren.

B – *Tweede vraag*

79. Met zijn tweede vraag wenst het Bundesgerichtshof te vernemen of artikel 7, onder f), van richtlijn 95/46 zich verzet tegen een regel van nationaal recht op grond waarvan persoonsgegevens van een gebruiker, zonder diens toestemming, enkel mogen worden verzameld en benut wanneer dit nodig is om het concrete gebruik van de elektronische mediadienst door de gebruiker mogelijk te maken en te factureren, en op grond waarvan de doelstelling die erin bestaat de goede werking van de dienst te waarborgen, niet rechtvaardigt dat de gegevens worden benut na afloop van het betrokken gebruik.

80. Het antwoord op deze vraag vereist een voorafgaande opmerking over de door het Bundesgerichtshof verstrekte informatie volgens welke de betrokken gegevens worden bewaard ter waarborging van de goede werking van de websites waarover het in het hoofdgeding gaat, welke gegevens eventueel strafvervolging mogelijk maken wanneer internetaanvallen op die sites worden uitgevoerd.

81. Eerst moet dus worden onderzocht of de verwerking van de IP-adressen waar de prejudiciële verwijzing betrekking op heeft, valt onder de uitzondering van artikel 3, lid 2, eerste streepje, van richtlijn 95/46.[23]

1. Is richtlijn 95/46 van toepassing op de verwerking van de betrokken gegevens?

82. De Bondsrepubliek Duitsland treedt in het hoofdgeding kennelijk enkel op als aanbieder van internetdiensten, dat wil zeggen als particulier (en dus sine imperio). Uit dat feit kan worden afgeleid dat de verwerking van de gegevens die in het hoofdgeding aan de orde zijn in beginsel niet van de toepassing van richtlijn 95/46 is uitgesloten.

83. Om het met de woorden van het Hof in het arrest Lindqvist[24] te zeggen, de activiteiten van artikel 3, lid 2, van richtlijn 95/46 zijn „telkens specifieke activiteiten van de staten of de overheidsdiensten [die] met de activiteiten van particulieren niets van doen [hebben]”.[25] Voor zover de verwerking van de betrokken gegevens geschiedt door een verantwoordelijke die, ondanks zijn hoedanigheid van overheidsorgaan, in feite optreedt als een particulier rechtssubject, is richtlijn 95/46 van toepassing.

84. De verwijzende rechter wijst erop dat de Duitse overheid met de opslag van de dynamische IP-adressen hoofdzakelijk beoogt „de veiligheid en de goede werking van haar elektronische mediadiensten te waarborgen en in stand te houden”, met name de herkenning en de afweer te vergemakkelijken van vaak voorkomende „denial-of-serviceaanvallen”, waarbij de elektronische media-infrastructuur door het gericht en gecoördineerd bestoken van afzonderlijke servers wordt ontwricht met een groot aantal aanvragen.[26] De opslag van dynamische IP-adressen met dat doel is voor elke eigenaar van een website van enige betekenis een heel gewone zaak en houdt noch direct, noch indirect, de uitoefening van openbaar gezag in. Daarom kan richtlijn 95/46 er zonder al te grote moeilijkheden op worden toegepast.

23 — Onder de toepassing van richtlijn 95/46 vallen niet „verwerkingen die betrekking hebben op de openbare veiligheid, defensie, de veiligheid van de staat [...] *en de activiteiten van de staat op strafrechtelijk gebied*” (cursivering van mij).

24 — Arrest van 6 november 2003 (C-101/01, EU:C:2003:596, punt 43).

25 — In dezelfde zin het arrest van 16 december 2008, Satakunnan Markkinapörssi en Satamedia (C-73/07, EU:C:2008:727, punt 41).

26 — Punt 36 van de verwijzingsbeschikking.

85. Het Bundesgerichtshof benadrukt echter dat de opslag van de dynamische IP-adressen door de aanbieders van de internetdiensten die in het hoofdgeding zijn betrokken, ook tot doel heeft te zijner tijd een strafrechtelijke actie in te stellen tegen daders van eventuele internetaanvallen. Is dat doel voldoende om de verwerking van die gegevens uit te sluiten van de werkingssfeer van richtlijn 95/46?

86. Naar mijn mening zouden wij, als onder „strafrechtelijke actie" de uitoefening van het ius puniendi van de Staat door de in het hoofdgeding gedaagde aanbieders van internetdiensten wordt verstaan, te maken hebben met „activiteiten van de Staat op strafrechtelijk gebied" en dus met een van de uitzonderingen van artikel 3, lid 2, eerste streepje, van richtlijn 95/46.

87. Onder die omstandigheden zou, volgens de rechtspraak van het Hof in de zaak Huber [27], de door de aanbieders van de diensten verrichte verwerking van persoonsgegevens ten behoeve van de veiligheid en de goede technische werking van hun elektronische mediadiensten, binnen de werkingssfeer van richtlijn 95/46 vallen, terwijl de verwerking van gegevens die gericht is op de activiteiten van de Staat op strafrechtelijk gebied, daarbuiten valt.

88. Op dezelfde wijze zou, ook wanneer de eigenlijke strafvervolging niet aan de Bondsrepubliek Duitsland toekomt – omdat deze enkel als aanbieder van internetdiensten zonder openbaar gezag optreedt, en zij net als elke andere particulier de betrokken IP-adressen slechts overdraagt aan een overheidsorgaan met het oog op strafvervolging – de verwerking van de dynamische IP-adressen een activiteit tot doel hebben die buiten de werkingssfeer van richtlijn 95/46 valt.

89. Dat blijkt uit de rechtspraak in de zaak Parlement/Raad en Commissie [28], waarin het Hof overwoog dat het feit dat bepaalde persoonsgegevens „door particuliere marktdeelnemers voor commerciële doeleinden zijn verzameld en het deze laatste zijn die ze doorgeven naar een derde land" niet betekent dat deze doorgifte „niet binnen de werkingssfeer" van artikel 3, lid 2, eerste streepje, van richtlijn 95/46 valt, wanneer het doel van de doorgifte betrekking heeft op de activiteiten van de Staat op strafrechtelijk gebied, omdat de doorgifte in deze zaak „geschiedt binnen een door de overheid ingesteld kader dat betrekking heeft op de openbare veiligheid". [29]

90. Als daarentegen – zoals ik denk, en zoals uit de verwijzingsbeschikking kan worden afgeleid – onder „strafrechtelijke actie" de actie moet worden verstaan van een particulier, die het recht heeft om de Staat middels de daartoe vastgestelde procedure te verzoeken zijn ius puniendi uit te oefenen, dan kan niet met succes worden gesteld dat de verwerking van de dynamische IP-adressen de activiteiten van de Staat op strafrechtelijk gebied tot doel heeft, die van de werkingssfeer van richtlijn 95/46 zijn uitgesloten.

91. De bewaring en de opslag van dat gegeven dienen dan namelijk als één van de bewijsmiddelen die de eigenaar van de website kan aandragen in het kader van zijn verzoek aan de Staat om vervolging van een onrechtmatige handeling. Het zou kortom een instrument zijn om, via het strafrecht, de rechten te beschermen die door de rechtsorde aan een bepaald rechtssubject (in dit geval een overheidsorgaan dat binnen het privaatrecht optreedt) zijn toegekend. Vanuit dat gezichtspunt bestaat er geen verschil met het initiatief van een willekeurige andere aanbieder van internetdiensten die verzoekt om bescherming van de Staat overeenkomstig de procedures voor de uitoefening van de strafvervolging zoals die in de rechtsorde zijn vastgesteld.

27 — Arrest van 16 december 2008 (C-524/06, EU:C:2008:724, punt 45).

28 — Arrest van 30 mei 2006 (C-317/04 en C-318/04, EU:C:2006:346, punten 54-59).

29 — Ibidem, punt 59. De zaak betrof persoonsgegevens waarvan de verwerking niet nodig was voor de verrichting van de diensten die de hoofdactiviteit waren van de betrokken private ondernemers (luchtvaartmaatschappijen) en die deze ondernemers aan de autoriteiten van de Verenigde Staten moesten doorgeven om terrorisme te voorkomen en te bestrijden.

92. Daarom valt, voor zover de Duitse overheid zich gedraagt als een aanbieder van internetdiensten zonder openbaar gezag – hetgeen de verwijzende rechter moet beoordelen – de verwerking die zij verricht van de dynamische IP-adressen, als persoonsgegevens, binnen de werkingssfeer van richtlijn 95/46.

2. Beantwoording van de vraag

93. § 15, lid 1, TMG staat het verzamelen en benutten van persoonsgegevens van een gebruiker slechts toe wanneer dit nodig is om een concreet gebruik van elektronische mediadiensten mogelijk te maken en te factureren. Preciezer gezegd, de aanbieder van de diensten kan enkel de zogeheten „gebruiksgegevens" verzamelen en benutten, dat wil zeggen de persoonsgegevens van een gebruiker die nodig zijn voor „het gebruik en de facturering van de elektronische mediadiensten." Deze gegevens moeten onmiddellijk na afloop van de sessie worden gewist (zodra het concrete gebruik van de elektronische mediadienst is beëindigd), tenzij zij moeten worden bewaard „wanneer zij voor de facturering nodig zijn", zoals § 15, lid 4, TMG bepaalt.

94. § 15 TMG schijnt uit te sluiten dat na beëindiging van de verbinding de gebruiksgegevens worden opgeslagen voor andere doeleinden, waaronder het doel „het gebruik van elektronische mediadiensten" in het algemeen te waarborgen. Omdat § 15 enkel het doel van facturering noemt als rechtvaardigingsgrond voor de bewaring van de gegevens, kan dat artikel worden gelezen (hoewel de definitieve uitlegging ervan de taak van de verwijzende rechter is) als een bepaling dat de gebruiksgegevens alleen mogen worden gebruikt om een concrete gebruiksverhouding mogelijk te maken, en dat zij gewist moeten worden na afloop daarvan.

95. Artikel 7, onder f), van richtlijn 95/46[30] staat de verwerking van persoonsgegevens mijns inziens toe in meer genereuze bewoordingen (voor de voor de verwerking verantwoordelijke) dan die van § 15 TMG. Op dit punt is de Duitse regeling strikter te noemen dan de Unieregeling, want de eerste erkent in beginsel geen ander gerechtvaardigd belang dan dat van de facturering van de dienst, terwijl de Bondsrepubliek Duitsland, als aanbieder van internetdiensten, ook een gerechtvaardigd belang zou kunnen hebben bij de waarborging van de goede werking van haar websites, naast elke gebruiksverhouding.[31]

96. De uitspraak van het Hof in het arrest ASNEF en FECEMD[32] zet de lijnen uit voor het antwoord op de tweede prejudiciële vraag. Het Hof oordeelde daarin dat uit het doel van richtlijn 95/46 voortvloeit „[...] dat artikel 7 van richtlijn 95/46 een uitputtende lijst bevat van gevallen waarin een verwerking van persoonsgegevens als rechtmatig kan worden aangemerkt".[33] Vandaar dat „de lidstaten aan artikel 7 van richtlijn 95/46 geen nieuwe beginselen betreffende de toelaatbaarheid van de verwerking van persoonsgegevens mogen toevoegen, noch bijkomende vereisten mogen vaststellen die de reikwijdte van een van de zes in dat artikel vervatte beginselen zouden wijzigen".[34]

97. Weliswaar voegt §15 TMG aan de voorwaarden van artikel 7 van richtlijn 95/46 voor de rechtmatigheid van gegevensverwerking geen nieuwe toe – zoals gebeurde in de zaken ASNEF en FECEMD[35] – maar als artikel 7 wordt uitgelegd in de door de verwijzende rechter bedoelde restrictieve zin, wordt de inhoud van de voorwaarde onder f) van dat artikel beperkt. Terwijl de Uniewetgever in

30 — Weergegeven in punt 17.

31 — Zie punt 84. Zonder twijfel hebben eigenaren van websites een wettelijk belang bij het voorkomen en bestrijden van de door de verwijzende rechter genoemde dos-aanvallen („denial of service"), namelijk massale gecoördineerde aanvallen die soms tegen websites worden gericht om ze te overspoelen en daardoor plat te leggen.

32 — Arrest van 24 november 2011 (C-468/10 en C-469/10, EU:C:2011:777).

33 — Ibidem, punt 30.

34 — Ibidem, punt 32.

35 — In die zaak voegde de nationale wetgever aan de voorwaarden van artikel 7, onder f), van richtlijn 95/46 als voorwaarde toe dat de te verwerken gegevens zijn opgenomen in voor het publiek toegankelijke bronnen.

algemene zin spreekt van de „behartiging van het gerechtvaardigde belang van de voor de verwerking verantwoordelijke of van de derde(n) aan wie de gegevens worden verstrekt", ziet § 15 TMG enkel op de noodzaak om „het [concrete] gebruik van elektronische mediadiensten mogelijk te maken en te factureren".

98. Net als in de zaken ASNEF en FECEMD [36] zou in de onderhavige zaak – als, nogmaals, artikel 7 in de hierboven uiteengezette beperkte zin zou worden uitgelegd – een nationale maatregel de werkingssfeer van een beginsel van artikel 7 van richtlijn 95/46 wijzigen, in plaats van enkel nader bepalen, hetgeen het enige is waartoe de autoriteiten van de lidstaten op grond van artikel 5 van richtlijn 95/46 een zekere beoordelingsmarge bezitten.

99. Volgens dat laatstgenoemde artikel „[bepalen] de lidstaten [...] binnen de grenzen van de bepalingen van dit hoofdstuk [37] nader de voorwaarden waaronder de verwerking van persoonsgegevens rechtmatig is". Het Hof overwoog echter in de zaken ASNEF en FECEMD [38] „dat de lidstaten krachtens artikel 5 van richtlijn 95/46 ook geen andere beginselen betreffende de toelaatbaarheid van de verwerking van persoonsgegevens mogen invoeren dan die welke worden genoemd in artikel 7 van die richtlijn, noch door middel van bijkomende vereisten de reikwijdte van de zes in voornoemd artikel 7 voorziene beginselen mogen wijzigen".

100. In verhouding tot artikel 7, onder f), van richtlijn 95/46 zou § 15 TMG de reikwijdte van het legitieme belang dat gegevensverwerking rechtvaardigt substantieel verkleinen, in plaats van deze reikwijdte slechts nader te bepalen of te nuanceren binnen de marge van hetgeen door artikel 5 van die richtlijn wordt toegestaan. § 15 zou dat bovendien categorisch en absoluut doen, zonder de mogelijkheid open te laten dat de bescherming en de waarborging van het algemene gebruik van de elektronische mediadienst worden afgewogen tegen „het belang of de fundamentele rechten en vrijheden van de betrokkene die aanspraak maakt op bescherming uit hoofde van artikel 1, lid 1," van richtlijn 95/46, zoals artikel 7, onder f), ervan verlangt.

101. Net als in de zaken ASNEF en FECEMD [39] heeft de Duitse federale wetgever [voor bepaalde categorieën persoonsgegevens] „de uitkomst van de afweging van tegengestelde rechten en belangen definitief [vastgesteld], zonder ruimte te bieden voor een afwijkende uitkomst wegens de bijzondere omstandigheden van een concreet geval", zodat „er geen sprake meer [is] van een nadere bepaling in de zin van [...] artikel 5" van richtlijn 95/46.

102. Onder deze omstandigheden ben ik van mening dat het Bundesgerichtshof verplicht is de nationale wettelijke regeling overeenkomstig richtlijn 95/46 uit te leggen, hetgeen betekent: a) dat tot de rechtvaardigingsgronden voor de verwerking van de zogeheten „gebruiksgegevens" ook het legitieme belang van de aanbieder van elektronische mediadiensten kan behoren, het algemeen gebruik van die diensten te waarborgen, en b) dat, per geval, dit belang van de aanbieder van de dienst moet worden afgewogen tegen het belang of de fundamentele rechten en vrijheden van de gebruiker, om te kunnen beoordelen welk daarvan valt onder de bescherming van artikel 1, lid 1, van richtlijn 95/46. [40]

36 — Arrest van 24 november 2011 (C-468/10 en C-469/10, EU:C:2011:777).

37 — Hoofdstuk II, met het opschrift „Algemene voorwaarden voor de rechtmatigheid van de verwerking van persoonsgegevens" dat de artikelen 5 tot en met 21 van richtlijn 95/46 omvat.

38 — Arrest van 24 november 2011 (C-468/10 en C-469/10, EU:C:2011:777, punt 36).

39 — Ibidem, punt 47.

40 — Tijdens de zitting heeft de raadsman van Breyer opgemerkt dat de opslag van de dynamische IP-adressen onnodig was voor de bescherming van de goede werking van de internetdiensten tegen eventuele aanvallen. Ik denk niet dat over die vraag een absolute uitspraak kan worden gedaan. Ik denk eerder dat elke uitspraak moet worden voorafgegaan door een afweging per geval tussen de belangen van de eigenaar van de website en de rechten en de belangen van de gebruikers.

103. Naar mijn mening behoeft verder niets te worden toegevoegd over de wijze waarop die afweging in de zaak waarop de prejudiciële verwijzing betrekking heeft, moet plaatsvinden. Het Bundesgerichtshof stelt over dat punt geen vraag, maar verzoekt om antwoord op een vraag die aan deze afweging voorafgaat, namelijk of die afweging mag plaatsvinden.

104. Het lijkt mij ten slotte overbodig op te merken dat de verwijzende rechter rekening kan houden met de eventuele wettelijke bepalingen die de lidstaat heeft aangenomen in het kader van de mogelijkheid om conform artikel 13, lid 1, onder d), van richtlijn 95/46 de omvang van de in artikel 6 van die richtlijn bedoelde rechten en verplichtingen te beperken, indien dat nodig is ter vrijwaring van, onder andere, „het voorkomen, het onderzoeken, opsporen en vervolgen van strafbare feiten [...]". Ook dat punt noemt de verwijzende rechter niet, terwijl hij zich toch zeker bewust zal zijn van het bestaan van beide artikelen.

105. Daarom geef ik in overweging om op de tweede prejudiciële vraag te antwoorden dat artikel 7, onder f), van richtlijn 95/46 zich verzet tegen een nationale bepaling waarvan de uitlegging een aanbieder van diensten verhindert om persoonsgegevens van een gebruiker zonder diens toestemming, na afloop van elk gebruik, te bewaren en te verwerken ter waarborging van de goede werking van de elektronische mediadienst.

VI – **Conclusie**

106. Op grond van het voorgaande geef ik het Hof in overweging de gestelde vragen te beantwoorden als volgt:

„1) Overeenkomstig artikel 2, onder a), van richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, vormt een dynamisch IP-adres waarmee een gebruiker toegang heeft gekregen tot de website van een aanbieder van elektronische mediadiensten voor deze laatste een ‚persoonsgegeven', wanneer een internetprovider beschikt over de aanvullende gegevens die het, samen met het dynamische IP-adres, mogelijk maken de gebruiker te identificeren.

2) Artikel 7, onder f), van richtlijn 95/46 moet aldus worden uitgelegd dat het doel, de goede werking van de elektronische mediadienst te waarborgen, in beginsel kan worden beschouwd als een legitiem belang dat de verwerking van het voornoemde persoonsgegeven rechtvaardigt, mits dat belang prevaleert boven het belang of de fundamentele rechten van de betrokkene. Een nationale bepaling volgens welke geen rekening kan worden gehouden met dat legitieme belang, is onverenigbaar met dat artikel."