СЪД НА ЕВРОПЕЙСКИЯ СЪЮЗ
TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA
SOUDNÍ DVŮR EVROPSKÉ UNIE
DEN EUROPÆISKE UNIONS DOMSTOL
GERICHTSHOF DER EUROPÄISCHEN UNION
EUROOPA LIIDU KOHUS
ΔΙΚΑΣΤΗΡΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ
COURT OF JUSTICE OF THE EUROPEAN UNION
COUR DE JUSTICE DE L'UNION EUROPÉENNE
CÚIRT BHREITHIÚNAIS AN AONTAIS EORPAIGH
SUD EUROPSKE UNIJE
CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA
EIROPAS SAVIENĪBAS TIESA
EUROPOS SĄJUNGOS TEISINGUMO TEISMAS
AZ EURÓPAI UNIÓ BÍRÓSÁGA
IL-QORTI TAL-ĠUSTIZZJA TAL-UNJONI EWROPEA
HOF VAN JUSTITIE VAN DE EUROPESE UNIE
TRYBUNAŁ SPRAWIEDLIWOŚCI UNII EUROPEJSKIEJ
TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA
CURTEA DE JUSTIȚIE A UNIUNII EUROPENE
SÚDNY DVOR EURÓPSKEJ ÚNIE
SODIŠČE EVROPSKE UNIJE
EUROOPAN UNIONIN TUOMIOISTUIN
EUROPEISKA UNIONENS DOMSTOL
CVRIA
LUXEMBOURG

SCHLUSSANTRÄGE DES GENERALANWALTS
MANUEL CAMPOS SÁNCHEZ-BORDONA
vom 12. Mai 2016[1]

Rechtssache C-582/14

Patrick Breyer
gegen
Bundesrepublik Deutschland

(Vorabentscheidungsersuchen des Bundesgerichtshofs, Deutschland)

„Verarbeitung personenbezogener Daten – Richtlinie 95/46/EG – Art. 2 Buchst. a und Art. 7 Buchst. f – Begriff ‚personenbezogeneDaten' – IP-Adressen – Speicherung durch einen Diensteanbieter für Telemedien – Nationale Regelung, die eine Berücksichtigung des berechtigten Interesses des für die Verarbeitung Verantwortlichen nicht zulässt"

[1] – Originalsprache: Spanisch.

1. Eine Internetprotokoll-Adresse (im Folgenden: IP-Adresse) ist eine Ziffernfolge aus binären Zahlen, die einem Gerät (einem Computer, einem Tablet oder einem Smartphone) zugewiesen wird, dieses identifiziert und ihm den Zugang zum elektronischen Kommunikationsnetz ermöglicht. Für eine Verbindung mit dem Internet muss das Gerät diese von den Internetzugangsanbietern vergebene Ziffernfolge verwenden. Die IP-Adresse wird an den Server übermittelt, auf dem die abgerufene Internetseite gespeichert ist.

2. Die Internetzugangsanbieter (im Allgemeinen die Telefongesellschaften) weisen ihren Kunden für jede Verbindung mit dem Internet für einen begrenzten Zeitraum sogenannte „dynamische IP-Adressen“ zu, die sich bei späteren Verbindungen ändern. Diese Gesellschaften führen ein Verzeichnis darüber, welche IP-Adresse sie zum jeweiligen Zeitpunkt einem bestimmten Gerät zugewiesen hatten[2].

3. Die Inhaber der Internetseiten, auf die mittels dynamischer IP-Adressen zugegriffen wird, führen gewöhnlich ebenfalls Verzeichnisse, in denen sie speichern, welche Seiten wann und von welcher dynamischen IP-Adresse aus aufgerufen wurden. Diese Verzeichnisse können technisch nach dem Ende der Internetverbindung des jeweiligen Nutzers unbefristet gespeichert werden.

4. Eine dynamische IP-Adresse reicht für sich allein nicht aus, damit der Diensteanbieter den Nutzer seiner Internetseite identifizieren kann. Dies kann er jedoch, wenn er die dynamische IP-Adresse mit anderen zusätzlichen Daten verbindet, über die der Internetzugangsanbieter verfügt.

5. Im Ausgangsverfahren wird darüber gestritten, ob dynamische IP-Adressen personenbezogene Daten im Sinne von Art. 2 Buchst. a der Richtlinie 95/46/EG[3] sind. Zur Beantwortung dieser Frage muss zunächst geklärt werden, welche Bedeutung dabei dem Umstand zukommt, dass die für die Identifizierung des Nutzers erforderlichen zusätzlichen Daten sich nicht im Besitz des Inhabers der Internetseite, sondern im Besitz eines Dritten (konkret des Internetzugangsanbieters) befinden.

[2] – Art. 5 der Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (ABl. 2006, L 105, S. 54) enthält unter anderem die Verpflichtung, zum Zweck der Ermittlung, Feststellung und Verfolgung schwerwiegender Verstöße „Datum und Uhrzeit der An- und Abmeldung beim Internetzugangsdienst, … zusammen mit der vom Internetzugangsanbieter einer Verbindung zugewiesenen dynamischen oder statischen IP-Adresse und die Benutzerkennung des Teilnehmers oder des registrierten Benutzers“ zu speichern.

[3] – Richtlinie des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. 1995, L 281, S. 31).

6. Diese Frage hat der Gerichtshof noch nicht entschieden. In Rn. 51 des Urteils Scarlet Extended[4] hat er zwar festgestellt, dass es sich bei IP-Adressen „um geschützte personenbezogene Daten handelt, da sie die genaue Identifizierung der Nutzer ermöglichen“, aber in einem Kontext, in dem die Speicherung und Identifizierung der IP-Adressen durch den Internetzugangsanbieter[5] erfolgte und nicht wie hier durch den Anbieter von Inhalten.

7. Falls die dynamischen IP-Adressen für den Internetdiensteanbieter personenbezogene Daten sind, ist anschließend zu prüfen, ob ihre Verarbeitung in den Anwendungsbereich der Richtlinie 95/46 fällt.

8. Möglicherweise genießen diese Adressen, obwohl sie personenbezogene Daten darstellen, nicht den Schutz der Richtlinie 95/46, wenn z. B. ihre Verarbeitung der Strafverfolgung möglicher Angriffe auf die Internetseite dient. In diesem Fall ist die Richtlinie 95/46 gemäß Art. 3 Abs. 2 erster Gedankenstrich nicht anwendbar.

9. Darüber hinaus ist zu klären, ob der Internetdiensteanbieter, der die dynamischen IP-Adressen speichert, wenn Nutzer seine Internetseiten abrufen (in dieser Rechtssache die Bundesrepublik Deutschland), in Ausübung öffentlicher Gewalt oder als Privatperson handelt.

10. Falls die Richtlinie 95/46 anwendbar ist, ist schließlich klarzustellen, inwieweit mit Art. 7 Buchst. f dieser Richtlinie eine nationale Regelung vereinbar ist, die die Tragweite einer der in dieser Bestimmung vorgesehenen Voraussetzungen für die Rechtfertigung der Verarbeitung personenbezogener Daten einschränkt.

I – Rechtlicher Rahmen

A – *Unionsrecht*

11. Der 26. Erwägungsgrund der Richtlinie 95/46 lautet wie folgt:

„(26) Die Schutzprinzipien müssen für alle Informationen über eine bestimmte oder bestimmbare Person gelten. Bei der Entscheidung, ob eine Person bestimmbar ist, sollten alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen. Die Schutzprinzipien finden keine Anwendung auf Daten, die derart anonymisiert sind, dass die betroffene Person nicht mehr identifizierbar ist. Die

4 – Urteil vom 24. November 2011 (C-70/10, EU:C:2011:771, Rn. 51).

5 – So auch im Urteil vom 19. April 2012, Bonnier Audio u. a. (C-461/10, EU:C:2012:219, Rn. 51 und 52).

Verhaltensregeln im Sinne des Artikels 27 können ein nützliches Instrument sein, mit dem angegeben wird, wie sich die Daten in einer Form anonymisieren und aufbewahren lassen, die die Identifizierung der betroffenen Person unmöglich macht."

12. Art. 1 der Richtlinie 95/46 sieht vor:

„(1) Die Mitgliedstaaten gewährleisten nach den Bestimmungen dieser Richtlinie den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten.

(2) Die Mitgliedstaaten beschränken oder untersagen nicht den freien Verkehr personenbezogener Daten zwischen Mitgliedstaaten aus Gründen des gemäß Absatz 1 gewährleisteten Schutzes."

13. Art. 2 der Richtlinie 95/46 bestimmt:

„Im Sinne dieser Richtlinie bezeichnen die Ausdrücke

a) ‚personenbezogene Daten' alle Informationen über eine bestimmte oder bestimmbare natürliche Person (‚betroffene Person'); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind;

b) ‚Verarbeitung personenbezogener Daten' (‚Verarbeitung') jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Speichern, die Organisation, die Aufbewahrung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Benutzung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, die Kombination oder die Verknüpfung sowie das Sperren, Löschen oder Vernichten.

…

d) ‚für die Verarbeitung Verantwortlicher' die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Sind die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten in einzelstaatlichen oder gemeinschaftlichen Rechts- und Verwaltungsvorschriften festgelegt, so können der für die Verarbeitung Verantwortliche bzw. die spezifischen

Kriterien für seine Benennung durch einzelstaatliche oder gemeinschaftliche Rechtsvorschriften bestimmt werden;

…

f) ‚Dritter' eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, außer der betroffenen Person, dem für die Verarbeitung Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters befugt sind, die Daten zu verarbeiten;

…"

14. Art. 3 („Anwendungsbereich") der Richtlinie 95/46 sieht vor:

„(1) Diese Richtlinie gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen.

(2) Diese Richtlinie findet keine Anwendung auf die Verarbeitung personenbezogener Daten:

– die für die Ausübung von Tätigkeiten erfolgt, die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen, beispielsweise Tätigkeiten gemäß den Titeln V und VI des Vertrags über die Europäische Union, und auf keinen Fall auf Verarbeitungen betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Verarbeitung die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich;

…"

15. Kapitel II („Allgemeine Bedingungen für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten") der Richtlinie 95/46 wird durch Art. 5 eingeleitet, der lautet: „Die Mitgliedstaaten bestimmen nach Maßgabe dieses Kapitels die Voraussetzungen näher, unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist."

16. Art. 6 der Richtlinie 95/46 bestimmt:

„(1) Die Mitgliedstaaten sehen vor, dass personenbezogene Daten

a) nach Treu und Glauben und auf rechtmäßige Weise verarbeitet werden;

b) für festgelegte eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise

weiterverarbeitet werden. Die Weiterverarbeitung von Daten zu historischen, statistischen oder wissenschaftlichen Zwecken ist im Allgemeinen nicht als unvereinbar mit den Zwecken der vorausgegangenen Datenerhebung anzusehen, sofern die Mitgliedstaaten geeignete Garantien vorsehen;

c) den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sind und nicht darüber hinausgehen;

d) sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht sind; es sind alle angemessenen Maßnahmen zu treffen, damit im Hinblick auf die Zwecke, für die sie erhoben oder weiterverarbeitet werden, nichtzutreffende oder unvollständige Daten gelöscht oder berichtigt werden;

e) nicht länger, als es für die Realisierung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist, in einer Form aufbewahrt werden, die die Identifizierung der betroffenen Personen ermöglicht. Die Mitgliedstaaten sehen geeignete Garantien für personenbezogene Daten vor, die über die vorgenannte Dauer hinaus für historische, statistische oder wissenschaftliche Zwecke aufbewahrt werden.

(2) Der für die Verarbeitung Verantwortliche hat für die Einhaltung des Absatzes 1 zu sorgen."

17. Art. 7 der Richtlinie 95/46 lautet:

„Die Mitgliedstaaten sehen vor, dass die Verarbeitung personenbezogener Daten lediglich erfolgen darf, wenn eine der folgenden Voraussetzungen erfüllt ist:

a) Die betroffene Person hat ohne jeden Zweifel ihre Einwilligung gegeben;

b) die Verarbeitung ist erforderlich für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder für die Durchführung vorvertraglicher Maßnahmen, die auf Antrag der betroffenen Person erfolgen;

c) die Verarbeitung ist für die Erfüllung einer rechtlichen Verpflichtung erforderlich, der der für die Verarbeitung Verantwortliche unterliegt;

d) die Verarbeitung ist erforderlich für die Wahrung lebenswichtiger Interessen der betroffenen Person;

e) die Verarbeitung ist erforderlich für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt und dem für die Verarbeitung Verantwortlichen oder dem Dritten, dem die Daten übermittelt werden, übertragen wurde;

f) die Verarbeitung ist erforderlich zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person, die gemäß Artikel 1 Absatz 1 geschützt sind, überwiegen."

18. Art. 13 der Richtlinie 95/46 bestimmt:

„(1) Die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Pflichten und Rechte gemäß Artikel 6 Absatz 1, Artikel 10, Artikel 11 Absatz 1, Artikel 12 und Artikel 21 beschränken, sofern eine solche Beschränkung notwendig ist für:

a) die Sicherheit des Staates;

b) die Landesverteidigung;

c) die öffentliche Sicherheit;

d) die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder Verstößen gegen die berufsständischen Regeln bei reglementierten Berufen;

e) ein wichtiges wirtschaftliches oder finanzielles Interesse eines Mitgliedstaats oder der Europäischen Union einschließlich Währungs-, Haushalts- und Steuerangelegenheiten;

f) Kontroll-, Überwachungs- und Ordnungsfunktionen, die dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt für die unter den Buchstaben c), d) und e) genannten Zwecke verbunden sind;

g) den Schutz der betroffenen Person und der Rechte und Freiheiten anderer Personen.

…"

B – *Nationales Recht*

19. § 12 Telemediengesetz (im Folgenden: TMG)[6] sieht vor:

„(1) Der Diensteanbieter darf personenbezogene Daten zur Bereitstellung von Telemedien nur erheben und verwenden, soweit dieses Gesetz oder eine andere Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht, es erlaubt oder der Nutzer eingewilligt hat.

[6] – Gesetz vom 26. Februar 2007 (BGBl. 2007 I, S. 179).

(2) Der Diensteanbieter darf für die Bereitstellung von Telemedien erhobene personenbezogene Daten für andere Zwecke nur verwenden, soweit dieses Gesetz oder eine andere Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht, es erlaubt oder der Nutzer eingewilligt hat.

(3) Soweit nichts anderes bestimmt ist, sind die jeweils geltenden Vorschriften für den Schutz personenbezogener Daten anzuwenden, auch wenn die Daten nicht automatisiert verarbeitet werden."

20. § 15 TMG lautet wie folgt:

„(1) Der Diensteanbieter darf personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen (Nutzungsdaten). Nutzungsdaten sind insbesondere

1. Merkmale zur Identifikation des Nutzers,

2. Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und

3. Angaben über die vom Nutzer in Anspruch genommenen Telemedien.

(2) Der Diensteanbieter darf Nutzungsdaten eines Nutzers über die Inanspruchnahme verschiedener Telemedien zusammenführen, soweit dies für Abrechnungszwecke mit dem Nutzer erforderlich ist.

…

(4) Der Diensteanbieter darf Nutzungsdaten über das Ende des Nutzungsvorgangs hinaus verwenden, soweit sie für Zwecke der Abrechnung mit dem Nutzer erforderlich sind (Abrechnungsdaten). Zur Erfüllung bestehender gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsfristen darf der Diensteanbieter die Daten sperren. …"

21. Gemäß § 3 Abs. 1 Bundesdatenschutzgesetz (im Folgenden: BDSG)[7] sind „[p]ersonenbezogene Daten … Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener) …"

II – Sachverhalt

22. Herr Breyer hat gegen die Bundesrepublik Deutschland Klage auf Unterlassung der Speicherung von IP-Adressen erhoben.

[7] – Gesetz vom 20. Dezember 1990 (BGBl. 1990 I, S. 2954).

23. Zahlreiche öffentliche Einrichtungen in Deutschland betreiben allgemein zugängliche Internetportale, auf denen sie aktuelle Informationen bereitstellen. Um Angriffe abzuwehren und die strafrechtliche Verfolgung von Angreifern zu ermöglichen, werden bei den meisten dieser Portale alle Zugriffe in Protokolldateien festgehalten. Darin werden auch über das Ende des jeweiligen Nutzungsvorgangs hinaus der Name der abgerufenen Datei bzw. Seite, in Suchfelder eingegebene Begriffe, der Zeitpunkt des Abrufs, die übertragene Datenmenge, die Feststellung des erfolgreichen Abrufs und die IP-Adresse des zugreifenden Rechners gespeichert.

24. Herr Breyer, der verschiedene solcher Seiten aufgerufen hat, beantragte, die Bundesrepublik Deutschland zu verurteilen, es zu unterlassen, die IP-Adresse des zugreifenden Hostsystems zu speichern oder durch Dritte speichern zu lassen, soweit die Speicherung nicht im Störungsfall zur Wiederherstellung der Verfügbarkeit des Telemediums erforderlich ist.

25. Die Klage von Herrn Breyer wurde im ersten Rechtszug abgewiesen. Seine Berufung hingegen hatte teilweise Erfolg, und die Bundesrepublik Deutschland wurde verurteilt, eine Speicherung über das Ende des jeweiligen Nutzungsvorgangs hinaus zu unterlassen. Die Unterlassungsanordnung wurde an die Voraussetzung geknüpft, dass der Kläger während des Nutzungsvorgangs seine Personalien, auch in Form einer E-Mail-Adresse, angibt, und dass die Speicherung nicht im Störungsfall zur Wiederherstellung der Verfügbarkeit des Telemediums erforderlich ist.

III – Vorlagefragen

26. Nachdem beide Parteien Revision eingelegt haben, hat der VI. Zivilsenat des Bundesgerichtshofs am 17. Dezember 2014 folgende Fragen zur Vorabentscheidung vorgelegt:

1. Ist Art. 2 Buchst. a der Richtlinie 95/46/EG dahin auszulegen, dass eine Internetprotokoll-Adresse (IP-Adresse), die ein Diensteanbieter im Zusammenhang mit einem Zugriff auf seine Internetseite speichert, für diesen schon dann ein personenbezogenes Datum darstellt, wenn ein Dritter (hier: Zugangsanbieter) über das zur Identifizierung der betroffenen Person erforderliche Zusatzwissen verfügt?

2. Steht Art. 7 Buchst. f der Datenschutz-Richtlinie einer Vorschrift des nationalen Rechts entgegen, wonach der Diensteanbieter personenbezogene Daten eines Nutzers ohne dessen Einwilligung nur erheben und verwenden darf, soweit dies erforderlich ist, um die konkrete Inanspruchnahme des Telemediums durch den jeweiligen Nutzer zu ermöglichen und abzurechnen, und wonach der Zweck, die generelle Funktionsfähigkeit des Telemediums zu gewährleisten, die Verwendung nicht über das Ende des jeweiligen Nutzungsvorgangs hinaus rechtfertigen kann?

27. Nach den Ausführungen des vorlegenden Gerichts könnte der Kläger nach deutschem Recht die Unterlassung der Speicherung der IP-Adressen verlangen, wenn deren Speicherung nach dem Datenschutzrecht einen unzulässigen Eingriff in sein allgemeines Persönlichkeitsrecht, genauer gesagt in sein Recht auf informationelle Selbstbestimmung (§ 1004 Abs. 1, § 823 Abs. 1 des Bürgerlichen Gesetzbuchs in Verbindung mit Art. 1 und 2 des Grundgesetzes), darstellen würde.

28. Dies wäre der Fall, wenn a) die IP-Adresse (jedenfalls zusammen mit dem Zeitpunkt des Zugriffs auf eine Internetseite) zu den „personenbezogenen Daten“ im Sinne von Art. 2 Buchst. a in Verbindung mit dem 26. Erwägungsgrund Satz 2 der Richtlinie 95/46 bzw. im Sinne von § 12 Abs. 1 und 3 TMG in Verbindung mit § 3 Abs. 1 BDSG zählte, und b) ein Erlaubnistatbestand im Sinne von Art. 7 Buchst. f der Richtlinie 95/46 bzw. im Sinne von § 12 Abs. 1 und 3 sowie § 15 Abs. 1 und 4 TMG nicht vorläge.

29. Dem Bundesgerichtshof zufolge ist es für die Auslegung des nationalen Rechts (§ 12 Abs. 1 TMG) entscheidend, wie der Personenbezug in Art. 2 Buchst. a der Richtlinie 95/46 zu verstehen ist.

30. Darüber hinaus dürfe, so führt das vorlegende Gericht aus, der Diensteanbieter gemäß § 15 Abs. 1 TMG personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit dies erforderlich sei, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen (Nutzungsdaten)[8]. Die Auslegung dieser nationalen Rechtsvorschrift hänge von der Auslegung des Art. 7 Buchst. f der Richtlinie 95/46 ab.

IV – Verfahren vor dem Gerichtshof und Vorbringen der Parteien

31. Schriftliche Erklärungen haben die deutsche, die österreichische und die portugiesische Regierung sowie die Kommission eingereicht. Zur mündlichen Verhandlung am 25. Februar 2016 sind nur die Kommission und Herr Breyer erschienen, während die deutsche Regierung auf eine Teilnahme verzichtet hat.

A – *Vorbringen der Beteiligten zur ersten Vorlagefrage*

32. Herr Breyer trägt vor, als personenbezogene Daten seien auch solche Daten anzusehen, deren Kombination nur theoretisch möglich sei, d. h. wenn von einer möglichen abstrakten Gefahr auszugehen sei, bei der es nicht darauf ankomme, ob die Daten in der Praxis tatsächlich kombiniert würden. Der Umstand, dass eine Stelle möglicherweise weitgehend außerstande sei, eine Person mittels ihrer IP-Adresse zu identifizieren, bedeute nicht, dass für diese Person eine solche Gefahr nicht bestehe. Darüber hinaus sei von Bedeutung, dass Deutschland seine IP-

[8] – Dem Bundesgerichtshof zufolge handelt es sich bei den Nutzungsdaten um die Merkmale zur Identifikation des Nutzers sowie um Angaben über Beginn, Ende und Umfang der Nutzung und über die vom Nutzer in Anspruch genommenen Telemedien.

Daten speichere, um gegebenenfalls Urheber etwaiger Angriffe zu identifizieren oder strafrechtlich zu verfolgen, was nach § 113 Telekommunikationsgesetz zulässig und oft geschehen sei.

33. Nach Ansicht der deutschen Regierung ist die erste Vorlagefrage zu verneinen. Dynamische IP-Adressen legten nicht die Identität einer „bestimmten" Person im Sinne von Art. 2 Buchst. a der Richtlinie 95/46 offen. Um zu entscheiden, ob sie Informationen über eine „bestimmbare" Person im Sinne dieser Vorschrift enthielten, müsse die Frage der *Bestimmbarkeit* nach einem „relativen" Maßstab geprüft werden. Dies ergebe sich aus dem 26. Erwägungsgrund der Richtlinie 95/46, nach dem nur die Mittel zu berücksichtigen seien, die „vernünftigerweise" entweder von dem für die Verarbeitung Verantwortlichen oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen. Damit werde klargestellt, dass der Unionsgesetzgeber solche Fälle nicht in den Anwendungsbereich der Richtlinie 95/46 habe einbeziehen wollen, in denen eine Identifizierung durch irgendeinen Dritten objektiv möglich sei.

34. Die deutsche Regierung ist darüber hinaus der Ansicht, dass der Begriff „personenbezogene Daten" im Sinne von Art. 2 Buchst. a der Richtlinie 95/46 entsprechend dem Zweck dieser Richtlinie, nämlich der Gewährleistung der Grundrechte, auszulegen sei. Das Schutzbedürfnis natürlicher Personen könne sich unterschiedlich darstellen, je nachdem, wer die Daten besitze und ob er über die Mittel verfüge, sie zur Identifizierung der Betroffenen einzusetzen.

35. Die Identität von Herrn Breyer lasse sich über die IP-Adresse in Verbindung mit den Zusatzinformationen, die von den Anbietern der Inhalte gespeichert würden, nicht feststellen. Dazu seien die Informationen erforderlich, über die die Internetzugangsanbieter verfügten, die diese aber den Anbietern der Inhalte nicht zugänglich machen dürften, weil es dafür keine gesetzliche Grundlage gebe.

36. Für die österreichische Regierung ist die Frage hingegen zu bejahen. Nach dem 26. Erwägungsgrund der Richtlinie 95/46 sei es für die Bestimmbarkeit einer Person nicht erforderlich, dass sich alle Daten zu ihrer Identifizierung in den Händen einer einzigen Stelle befänden. So könne eine IP-Adresse als personenbezogenes Datum anzusehen sein, wenn ein Dritter (wie z. B. der Internetzugangsanbieter) über die Mittel verfüge, um den Inhaber dieser Adresse ohne unverhältnismäßigen Aufwand zu identifizieren.

37. Die portugiesische Regierung neigt ebenfalls dazu, die Frage zu bejahen. Nach ihrer Auffassung stellt die IP-Adresse in Verbindung mit dem Zeitpunkt des Abfragevorgangs ein personenbezogenes Datum dar, soweit sie zur Identifizierung des Nutzers durch eine andere Stelle als die, die die IP-Adresse speichere, führen könne.

38. Die Kommission schlägt ebenfalls vor, die Frage zu bejahen, und stützt sich dabei auf die Entscheidung des Gerichtshofs in der Rechtssache Scarlet Extended[9]. Da die Speicherung der IP-Adressen gerade dazu diene, im Fall von Cyberangriffen die Nutzer zu identifizieren, stelle die Verwendung der von den Internetzugangsanbietern gespeicherten zusätzlichen Daten ein Mittel dar, das im Sinne des 26. Erwägungsgrundes der Richtlinie 95/46 „vernünftigerweise" eingesetzt werden könne. Letzten Endes sprechen nach Auffassung der Kommission sowohl der mit dieser Richtlinie verfolgte Zweck als auch Art. 7 und 8 der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta) für eine weite Auslegung von Art. 2 Buchst. a der Richtlinie 95/46.

B – *Vorbringen der Beteiligten zur zweiten Vorlagefrage*

39. Herr Breyer ist der Ansicht, dass Art. 7 Buchst. f der Richtlinie 95/46 eine Generalklausel darstelle, die zu ihrer praktischen Umsetzung einer Konkretisierung bedürfe. Im Einklang mit der Rechtsprechung des Gerichtshofs müssten daher die Umstände des konkreten Einzelfalls gewürdigt und festgestellt werden, ob es Gruppen mit einem berechtigten Interesse im Sinne dieser Vorschrift gebe. Wenn dies der Fall sei, sei es nicht nur zulässig, sondern für die Anwendung dieses Artikels sogar unabdingbar, Spezialregelungen für diese Gruppen vorzusehen. Im vorliegenden Fall sei die nationale Regelung mit Art. 7 Buchst. f der Richtlinie 95/46 vereinbar, da kein Interesse des Anbieters des öffentlichen Portals an der Speicherung personenbezogener Daten bestehe bzw. das Interesse am Schutz der Anonymität überwiege. Eine systematische personenbezogene Speicherung der Daten sei jedoch mit einer demokratischen Gesellschaft nicht vereinbar und weder erforderlich noch angemessen, um die Funktionsfähigkeit von Telemedien zu gewährleisten, was durchaus ohne eine Speicherung solcher personenbezogener Daten möglich sei, wie die Internetseiten einiger Bundesministerien zeigten.

40. Die deutsche Regierung macht geltend, die zweite Frage müsse nicht beantwortet werden, weil sie lediglich für den Fall gestellt worden sei, dass die erste Frage zu bejahen sei, was ihrer Ansicht nach aus den zuvor genannten Gründen nicht der Fall sei.

41. Die österreichische Regierung schlägt als Antwort vor, dass die Richtlinie 95/46 der Speicherung solcher wie der hier streitgegenständlichen Daten nicht allgemein entgegenstehe, sofern sie zur Gewährleistung der ordnungsgemäßen Funktionsfähigkeit der Telemedien unabdingbar sei. Eine begrenzte Speicherung der IP-Adresse über die Dauer des Abrufs einer Internetseite hinaus könne im Hinblick auf die Verpflichtung des für die Verarbeitung personenbezogener Daten Verantwortlichen, die sich aus Art. 17 Abs. 1 der Richtlinie 95/46 ergebenden Maßnahmen zum Schutz solcher Daten anzuwenden, rechtmäßig sein. Der Kampf gegen Cyberangriffe könne es rechtfertigen, Daten, die sich auf frühere Angriffe

9 – Urteil vom 24. November 2011 (C-70/10, EU:C:2011:771, Rn. 51).

bezögen, zu analysieren und bestimmten IP-Adressen den Zugriff auf die Internetseite zu verweigern. Die Verhältnismäßigkeit der Speicherung von Daten wie denen im Ausgangsverfahren in Rede stehenden müsse unter dem Blickwinkel des Zwecks, die ordnungsgemäße Funktionsfähigkeit der Telemedien zu gewährleisten, und unter Berücksichtigung der in Art. 6 Abs. 1 der Richtlinie 95/46 genannten Grundsätze jeweils im Einzelfall geprüft werden.

42. Die portugiesische Regierung steht auf dem Standpunkt, dass Art. 7 Buchst. f der Richtlinie 95/46 den im Ausgangsverfahren streitigen nationalen Rechtsvorschriften nicht entgegenstehe, weil der deutsche Gesetzgeber die in dieser Vorschrift vorgeschriebene Interessenabwägung zwischen den berechtigten Interessen des für die Verarbeitung personenbezogener Daten Verantwortlichen einerseits und den Rechten und Freiheiten der Inhaber dieser Daten andererseits bereits vorgenommen habe.

43. Die Kommission vertritt die Auffassung, die nationale Regelung, die Art. 7 Buchst. f der Richtlinie 95/46 umsetze, müsse die Zwecke der Verarbeitung personenbezogener Daten so festlegen, dass sie für den betroffenen Einzelnen vorhersehbar seien. Die deutsche Regelung erfülle diese Voraussetzung nicht, da sie in § 15 Abs. 1 TMG vorsehe, dass die Speicherung von IP-Adressen gestattet sei, „soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen“.

44. Die Kommission schlägt daher vor, die zweite Frage dahin zu beantworten, dass Art. 7 Buchst. f einer Auslegung einer nationalen Vorschrift entgegenstehe, wonach ein als Diensteanbieter tätiger Hoheitsträger personenbezogene Daten eines Nutzers ohne dessen Einwilligung auch mit dem Zweck erheben und verwenden dürfe, die generelle Funktionsfähigkeit des Telemediums zu gewährleisten, wenn die nationale Vorschrift diesen Zweck nicht hinreichend klar und präzise festlege.

V – Würdigung

A – *Erste Frage*

1. Abgrenzung der Vorlagefrage

45. Nach der vom Bundesgerichtshof gewählten Formulierung soll mit der ersten Vorlagefrage geklärt werden, ob eine IP-Adresse, mit der auf eine Internetseite zugegriffen wird, für die öffentliche Stelle, die Inhaberin dieser Seite ist, ein personenbezogenes Datum (im Sinne von Art. 2 Buchst. a der Richtlinie 95/46/EG) darstellt, wenn der Internetzugangsanbieter über das zur Identifizierung des Betroffenen erforderliche Zusatzwissen verfügt.

46. Die Frage ist hinreichend präzise formuliert, um andere Fragen zur Rechtsnatur von IP-Adressen, die sich *abstrakt* stellen könnten, im

Zusammenhang mit dem Schutz personenbezogener Daten von vornherein auszuschließen.

47. Erstens bezieht sich der Bundesgerichtshof ausschließlich auf „dynamische IP-Adressen“, d. h. auf solche, die für einen begrenzten Zeitraum für die jeweilige Verbindung mit dem Internet zugewiesen und bei späteren Verbindungen wieder geändert werden. Die sogenannten „festen“ oder „statischen“ IP-Adressen, die unveränderlich sind und die dauerhafte Identifizierung des mit dem Netz verbundenen Geräts ermöglichen, bleiben somit außer Betracht.

48. Zweitens geht das vorlegende Gericht von der Annahme aus, dass der Anbieter der Internetseite im Ausgangsverfahren weder dazu in der Lage ist, über die dynamische IP-Adresse festzustellen, wer seine Seiten besucht, noch selbst über die zusätzlichen Daten verfügt, die ihm in Verbindung mit der IP-Adresse die Identifizierung dieser Person ermöglichen würden. Der Bundesgerichtshof ist offensichtlich der Auffassung, dass die dynamische IP-Adresse in diesem Kontext *für den Anbieter der Internetseite* kein personenbezogenes Datum im Sinne von Art. 2 Buchst. a der Richtlinie 95/46 ist.

49. Die Zweifel des vorlegenden Gerichts betreffen die Frage, ob die dynamische IP-Adresse für den Anbieter der Internetseite ein personenbezogenes Datum darstellen kann, *wenn ein Dritter über das Zusatzwissen verfügt*, das in Verbindung mit der IP-Adresse die Identifizierung der Personen ermöglicht, die seine Internetseiten aufrufen. Dabei bezieht sich der Bundesgerichtshof, was eine weitere wichtige Klarstellung ist, nicht auf irgendeinen Dritten, der im Besitz von zusätzlichen Daten ist, sondern nur auf den Internetzugangsanbieter (womit er andere, die möglicherweise über derartige Daten verfügen, ausschließt).

50. So sind u. a. die folgenden Fragen nicht Gegenstand der Erörterung: a) Sind statische IP-Adressen personenbezogene Daten im Sinne der Richtlinie 95/46[10]? b) Sind dynamische IP-Adressen immer und unter allen Umständen personenbezogene Daten im Sinne dieser Richtlinie? c) Sind schließlich dynamische IP-Adressen unvermeidlich als personenbezogene Daten zu qualifizieren, sobald ein Dritter, wer dies auch sei, in der Lage ist, sie zur Identifizierung von Internetnutzern zu verwenden?

51. Es geht also einzig und allein um die Feststellung, ob eine dynamische IP-Adresse für den Anbieter eines Internetdienstes ein personenbezogenes Datum ist,

[10] – Diese Frage wurde vom Gerichtshof bereits in den Urteilen vom 24. November 2011, Scarlet Extended (C-70/10, EU:C:2011:771, Rn. 51), und vom 19. April 2012, Bonnier Audio u. a. (C-461/10, EU:C:2012:219), entschieden. In den Rn. 51 und 52 des letztgenannten Urteils stellte der Gerichtshof fest, dass die Auskunft „über den Namen und die Adresse eines Internetteilnehmers oder -nutzers …, der eine IP-Adresse nutzt, von der aus vermutlich Dateien mit geschützten Werken unrechtmäßig getauscht wurden, [um] … ihn identifizieren [zu] können[,] … eine Verarbeitung personenbezogener Daten im Sinne von Art. 2 Abs. 1 der Richtlinie 2002/58 in Verbindung mit Art. 2 Buchst. b der Richtlinie 95/46 darstellt“.

wenn die Telekommunikationsgesellschaft, die den Internetzugang anbietet (der Zugangsanbieter) zusätzliche Daten in Händen hat, die in Verbindung mit der fraglichen IP-Adresse die Identifizierung der Person ermöglichen, die die vom Diensteanbieter betriebene Internetseite aufruft.

2. Zur Beantwortung der Frage

52. Die in diesem Vorabentscheidungsersuchen aufgeworfene Frage ist in der deutschen Lehre und Rechtsprechung sehr umstritten, wobei sich zwei Meinungen gegenüber stehen[11]. Nach der einen (die einen „objektiven“ oder „absoluten“ Ansatz verfolgt) ist ein Nutzer bestimmbar – und damit die IP-Adresse ein schutzwürdiges personenbezogenes Datum –, wenn dessen Identifizierung unabhängig von den Möglichkeiten und Mitteln des Internetdiensteanbieters allein durch die Verbindung der dynamischen IP-Adresse mit von einem Dritten (z. B. dem Internetzugangsanbieter) bereitgestellten Daten möglich ist.

53. Für die Vertreter der anderen Auffassung (die einen „relativen“ Ansatz vertreten) reicht die Möglichkeit, sich zum Zweck der endgültigen Identifizierung des Nutzers der Hilfe eines Dritten zu bedienen, nicht aus, um bei einer dynamischen IP-Adresse den Personenbezug zu bejahen. Entscheidend sei, dass derjenige, der Zugang zu dem Datum habe, von diesem mit eigenen Mitteln Gebrauch machen und auf diese Weise jemanden identifizieren könne.

54. Ungeachtet dieses Meinungsstreits im nationalen Recht muss sich die Antwort des Gerichtshofs darauf beschränken, die beiden Bestimmungen der Richtlinie 95/46 auszulegen, auf die sich sowohl das vorlegende Gericht als auch die Parteien des Rechtsstreits beziehen, d. h. Art. 2 Buchst. a[12] und der 26. Erwägungsgrund[13].

55. Dynamische IP-Adressen legen allein dadurch, dass sie Informationen über Datum und Uhrzeit des Zugriffs von einem Computer (oder von einem anderen Gerät) auf eine Internetseite liefern, bestimmte Verhaltensmuster von Internetnutzern offen und stellen deshalb einen möglichen Eingriff in das Recht

[11] – Zu den beiden Lehrmeinungen siehe z. B. Schreibauer, M., in *Kommentar zum Bundesdatenschutzgesetz. Nebengesetze*, Esser, M., Kramer, P., und von Lewinski, K. (Hrsg.), Carl Heymanns Verlag/Wolters Kluwer, Köln, 2014, 4. Aufl., § 11 Telemediengesetz (4 bis 10). Nink, J., und Pohle, J., „Die Bestimmbarkeit des Personenbezugs. Von der IP-Adresse zum Anwendungsbereich der Datenschutzgesetze“, in *Multimedia und Recht*, 9/2015, S. 563 bis 567. Heidrich, J., und Wegener, C., „Rechtliche und technische Anforderungen an die Protokollierung von IT-Daten. Problemfall Logging“, in *Multimedia und Recht*, 8/2015, S. 487 bis 492. Leisterer, H., „Die neuen Pflichten zur Netz- und Informationssicherheit und die Verarbeitung personenbezogener Daten zur Gefahrenabwehr“, in *Computer und Recht*, 10/2015, S. 665 bis 670.

[12] – In Nr. 13 angeführt.

[13] – In Nr. 11 angeführt.

auf Achtung des Privatlebens dar[14], das in Art. 8 der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten und in Art. 7 der Charta gewährleistet ist, so dass die Richtlinie 95/46 in deren Licht sowie im Licht von Art. 8 der Charta auszulegen ist[15]. Tatsächlich ziehen die Parteien des Rechtsstreits diese Prämisse nicht in Zweifel, die als solche auch nicht Gegenstand der Vorlagefrage ist.

56. Die Person, auf die sich die genannten einzelnen Angaben beziehen, ist keine „bestimmte natürliche Person". Das Datum und die Uhrzeit einer Verbindung sowie ihr numerischer Ursprung lassen weder unmittelbar noch sofort erkennen, wer die natürliche Person ist, der das Gerät gehört, von dem aus die Internetseite besucht wird, und auch nicht die Identität des Nutzers, der es bedient (dies kann irgendeine natürliche Person sein).

57. Dennoch kann eine dynamische IP-Adresse, soweit sich mit ihrer Hilfe – allein oder in Verbindung mit anderen Daten – feststellen lässt, wer der Eigentümer des für den Zugang zu der Internetseite verwendeten Geräts ist, als eine Information über eine „bestimmbare Person" angesehen werden[16].

58. Nach Auffassung des Bundesgerichtshofs reicht eine dynamische IP-Adresse für sich allein nicht aus, um den Nutzer zu identifizieren, der mit ihr eine Internetseite aufgerufen hat. Könnte der Internetdiensteanbieter dagegen anhand

[14] – Darauf hat Generalanwalt Cruz Villalón in seinen Schlussanträgen in der Rechtssache Scarlet Extended (C-70/10, EU:C:2011:255, Nr. 76), hingewiesen, und so sieht es auch der Europäische Datenschutzbeauftragte in seinen Stellungnahmen vom 22. Februar 2010 zu den laufenden Verhandlungen der Europäischen Union über ein Abkommen zur Bekämpfung von Produkt- und Markenpiraterie (Anti-Counterfeiting Trade Agreement, ACTA) (ABl. 2010, C 147, S. 1, Rn. 24), und vom 10. Mai 2010 zum Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie von Kinderpornografie und zur Aufhebung des Rahmenbeschlusses 2004/68/JI (ABl. 2010, C 323, S. 6, Rn. 11).

[15] – Vgl. in diesem Sinne Urteil vom 20. Mai 2003, Österreichischer Rundfunk (C-465/00, C-138/01 und C-139/01, EU:C:2003:294, Rn. 68), und die Schlussanträge der Generalanwältin Kokott in der Rechtssache Promusicae (C-275/06, EU:C:2007:454, Nrn. 51 ff).

[16] – Bis zum Beweis des Gegenteils ist zu vermuten, dass es diese Person gewesen ist, die im Internet gesurft und die entsprechende Internetseite aufgerufen hat. Somit ermöglichen, abgesehen von dieser Vermutung, die Informationen über das Datum, die Uhrzeit und den numerischen Ursprung des Zugriffs auf eine Internetseite diesen Zugriff mit dem Eigentümer des Geräts in Verbindung zu bringen und indirekt einen Bezug zu seinem Verhalten im Netz herzustellen. Eine denkbare Ausnahme sind IP-Adressen, die Computern in Räumlichkeiten wie Internetcafés zugewiesen werden, deren anonyme Nutzer nicht bestimmbar sind und über deren Inhaber der Datenverkehr in diesen Räumlichkeiten keinerlei relevante personenbezogene Informationen liefert. Dies ist im Übrigen die einzige Ausnahme von dem Grundsatz, dass IP-Adressen personenbezogene Daten sind, die die mit der Richtlinie 95/46 eingesetzte Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten (die sogenannte „Artikel 29-Gruppe") akzeptiert hat. Ihre Stellungnahme 4/2007 vom 20. Juni 2007 zum Begriff „personenbezogene Daten", WP 136, findet sich auf http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

der dynamischen IP-Adresse den Nutzer identifizieren, wäre diese ganz eindeutig als ein personenbezogenes Datum im Sinne der Richtlinie 95/46 anzusehen. Darauf scheint allerdings die Vorlagefrage nicht abzuzielen, in der davon ausgegangen wird, dass die Internetdiensteanbieter, um die es im Ausgangsverfahren geht, den Nutzer nicht allein anhand der dynamischen IP-Adresse identifizieren können.

59. In Verbindung mit anderen Daten ermöglicht die dynamische IP-Adresse eine „indirekte" Identifizierung des Nutzers. In diesem Punkt sind sich alle einig. Erlaubt nun das eventuelle Vorhandensein solcher zusätzlicher Daten, die mit der dynamischen IP-Adresse verbunden werden können, ohne Weiteres deren Einstufung als personenbezogenes Datum im Sinne der Richtlinie? Es wird zu klären sein, ob dazu die bloß abstrakte Möglichkeit der Kenntnis von diesen Daten ausreicht oder ob vielmehr erforderlich ist, dass sie für denjenigen, der bereits die dynamische IP-Adresse kennt, oder für einen Dritten verfügbar sind.

60. Die Parteien konzentrieren sich in ihren Erklärungen auf die Auslegung des 26. Erwägungsgrundes der Richtlinie 95/46 und stellen dabei auf dessen Formulierung „Mittel …, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen", ab. Die Frage des vorlegenden Gerichts bezieht sich nicht auf zusätzliche Daten in den Händen der im Ausgangsverfahren betroffenen Diensteanbieter. Auch geht es nicht um irgendeinen Dritten, der über diese zusätzlichen Daten (die in Verbindung mit der dynamischen IP-Adresse die Bestimmung des Nutzers ermöglichen) verfügt, sondern um den Internetzugangsanbieter.

61. In diesem Fall ist also nicht erforderlich, dass der Gerichtshof sämtliche Mittel prüft, die die Beklagte des Ausgangsverfahrens „vernünftigerweise" einsetzen könnte, damit die dynamischen IP-Adressen, über die sie verfügt, als personenbezogene Daten qualifiziert werden können. Da der Bundesgerichtshof sich ausschließlich auf Zusatzwissen in den Händen Dritter bezieht, folgt daraus, dass a) entweder die Beklagte nicht über eigenes für die Bestimmung des Nutzers erforderliches Zusatzwissen verfügt oder b) sie, falls sie Zugang zu derartigem Wissen hat, nicht in der Lage ist, es als für die Verarbeitung Verantwortliche gemäß dem 26. Erwägungsgrund der Richtlinie 95/46 vernünftigerweise zu diesem Zweck einzusetzen.

62. Beide Annahmen hängen von tatsächlichen Feststellungen ab, für die ausschließlich das vorlegende Gericht zuständig ist. Der Gerichtshof könnte ihm allgemeine Hinweise zur Auslegung der Formulierung „Mittel …, die vernünftigerweise … von dem Verantwortlichen für die Verarbeitung … eingesetzt werden könnten" geben, wenn der Bundesgerichtshof Zweifel hätte, ob die Beklagte vernünftigerweise eigenes Zusatzwissen verwenden könnte. Da dies aber nicht der Fall ist, wäre es meiner Ansicht nach fehl am Platz, wenn der

Gerichtshof jetzt Auslegungskriterien festlegen würde, die für das vorlegende Gericht nicht unerlässlich sind und um die es auch nicht gebeten hat.

63. Somit geht es bei der vorgelegten Frage im Kern darum, ob es für die Qualifizierung dynamischer IP-Adressen als personenbezogene Daten von Bedeutung ist, dass ein ganz bestimmter Dritter, nämlich der Internetzugangsanbieter, über zusätzliche Daten verfügt, die in Verbindung mit diesen Adressen die Identifizierung des Nutzers ermöglichen, der eine bestimmte Internetseite besucht hat.

64. Erneut ist auf den 26. Erwägungsgrund der Richtlinie 95/46 zu verweisen. Die Formulierung „Mittel …, die vernünftigerweise … *von einem Dritten* eingesetzt werden könnten“[17], könnte dahin ausgelegt werden, dass es ausreicht, dass irgendein Dritter zusätzliche Daten erlangen kann (die zur Identifizierung einer Person mit einer dynamischen IP-Adresse verbunden werden können), damit eine solche Adresse *eo ipso* als personenbezogenes Datum anzusehen ist.

65. Diese weitestmögliche Auslegung würde in der Praxis dazu führen, dass jede Art von Information als personenbezogenes Datum einzuordnen wäre, so unzureichend sie für sich genommen auch wäre, um einen Nutzer bestimmen zu können. Niemals wird sich mit absoluter Sicherheit ausschließen lassen, dass es nicht einen Dritten gibt, der im Besitz von Zusatzwissen ist, das mit der fraglichen Information verbunden werden kann und es damit ermöglicht, die Identität einer Person festzustellen.

66. Die Möglichkeit, dass die Weiterentwicklung der technischen Mittel in einer mehr oder weniger nahen Zukunft den Zugang zu immer ausgefeilteren Instrumenten für die Gewinnung und Verarbeitung von Daten merklich vereinfachen wird, rechtfertigt meiner Ansicht nach die Schutzmaßnahmen, mit denen die Privatsphäre schon im Voraus geschützt werden soll. Es ist darauf geachtet worden, bei der Festlegung der einschlägigen rechtlichen Kategorien im Bereich des Datenschutzes hinreichend weit und flexibel gefasste Verhaltensweisen zu erfassen, um jede vorstellbare Fallgestaltung abdecken zu können[18].

67. Nichtsdestotrotz denke ich, dass diese – im Übrigen sehr berechtigte – Sorge nicht dazu führen kann, den Wortlaut, der den Willen des Gesetzgebers zum Ausdruck bringt, unbeachtet zu lassen, und dass die systematische Auslegung des 26. Erwägungsgrundes der Richtlinie 95/46 sich auf „Mittel …, die

[17] – Hervorhebung nur hier.

[18] – Auf diese Schutz- und Präventivfunktion stützt, wie ich ausgeführt habe, die Artikel 29-Gruppe ihren Standpunkt, dass IP-Adressen grundsätzlich personenbezogene Daten seien. Ausgenommen sei einzig der Fall, dass der Diensteanbieter mit absoluter Sicherheit sagen kann, dass die IP-Adressen zu nicht identifizierbaren Personen gehörten, wie es bei den Nutzern eines Internetcafés vorkommen könne. Vgl. Fn. 16 am Ende.

vernünftigerweise … *von bestimmten Dritten* eingesetzt werden könnten“, beschränkt.

68. Ebenso wie der 26. Erwägungsgrund nicht jedes Mittel einschließt, das der für die Verarbeitung Verantwortliche (in diesem Fall der Internetdiensteanbieter) einsetzen könnte, sondern nur jene, die dieser „vernünftigerweise“ einsetzen könnte, ist auch davon auszugehen, dass sich der Gesetzgeber auf „Dritte“ bezieht, an die sich der für die Verarbeitung Verantwortliche, der in den Besitz des für die Identifizierung erforderlichen Zusatzwissens gelangen möchte, *ebenfalls vernünftigerweise* wenden könnte. Das ist nicht der Fall, wenn der Kontakt mit diesen Dritten faktisch einen sehr hohen personellen und wirtschaftlichen Aufwand erfordern würde oder wenn er praktisch nicht durchführbar oder gesetzlich verboten wäre. Anderenfalls wäre es, wie schon dargelegt, praktisch unmöglich, zwischen den verschiedenen Mitteln zu unterscheiden, weil immer denkbar ist, dass es einen Dritten gibt, so unerreichbar er für den Internetdiensteanbieter auch sein mag, der – jetzt oder in Zukunft – über zusätzliche einschlägige Daten verfügt, die zur Identifizierung eines Nutzers beitragen können.

69. Wie ich bereits vorausgeschickt habe, handelt es sich bei dem vom Bundesgerichtshof in Bezug genommenen Dritten um einen Internetzugangsanbieter. Dieser ist sicherlich der Dritte, an den vernünftigerweise zuerst zu denken ist, wenn es darum geht, an wen der Diensteanbieter sich wenden kann, um die erforderlichen zusätzlichen Daten zu erhalten, wenn er möglichst effizient, praktisch und unmittelbar den Nutzer identifizieren will, der mit Hilfe einer dynamischen IP-Adresse seine Internetseite abgerufen hat. Es geht also keineswegs um einen hypothetischen, unbekannten und unerreichbaren Dritten, sondern um einen der Hauptakteure im Geflecht des Internets, von dem man mit Sicherheit weiß, dass er im Besitz der Daten ist, die der Diensteanbieter braucht, um einen Nutzer zu identifizieren. Tatsächlich ist es, wie das vorlegende Gericht ausführt, dieser bestimmte Dritte, an den sich die Beklagte des Ausgangsverfahrens wenden möchte, um das von ihr unbedingt benötigte Zusatzwissen zu erhalten.

70. Der Internetzugangsanbieter ist typischerweise der Dritte, auf den sich der 26. Erwägungsgrund der Richtlinie 95/46 bezieht und an den sich der Diensteanbieter im Ausgangsverfahren „am vernünftigsten“ wenden könnte. Es bleibt jedoch zu klären, ob es „vernünftigerweise“ durchführbar oder praktikabel ist, die zusätzlichen Daten zu beschaffen, die sich im Besitz dieses Dritten befinden.

71. Nach Ansicht der deutschen Regierung darf der Internetzugangsanbieter die Informationen, über die er verfüge – da sie personenbezogene Daten seien –, nicht

ohne Weiteres, sondern nur im Einklang mit den gesetzlichen Vorschriften über die Verarbeitung solcher Daten zugänglich machen[19].

72. Dies ist zweifellos richtig. Diese Informationen dürfen nur genutzt werden, wenn die Gesetze über personenbezogene Daten eingehalten werden. Eine Information kann nur „vernünftigerweise" erlangt werden, wenn die Voraussetzungen für den Zugang zu dieser Art Daten erfüllt sind. Erste Voraussetzung ist die gesetzliche Möglichkeit ihrer Speicherung und Weitergabe an andere. Natürlich ist der Internetzugangsanbieter berechtigt, die Herausgabe der betreffenden Daten zu verweigern, aber auch das Gegenteil ist möglich. Allein schon die durchaus „vernünftige" Möglichkeit einer Übermittlung von Daten macht nach dem Wortlaut des 26. Erwägungsgrundes der Richtlinie 95/46 aus der dynamischen IP-Adresse für den Internetdiensteanbieter ein personenbezogenes Datum.

73. Es handelt sich um eine Möglichkeit, die *im Rahmen des Gesetzes* realisierbar und deshalb „vernünftig" ist. Die vernünftigen Zugangsmöglichkeiten, auf die sich die Richtlinie 95/46 bezieht, müssen definitionsgemäß rechtmäßig sein[20]. Von dieser Prämisse geht natürlich das vorlegende Gericht aus, wie die deutsche Regierung in Erinnerung ruft[21]. So reduzieren sich die rechtlich relevanten Zugangsmöglichkeiten erheblich, weil ausschließlich die rechtmäßigen in Betracht kommen. Aber soweit es sie gibt – so beschränkt sie in ihrer praktischen Anwendung auch sein mögen –, stellen sie ein „vernünftiges Mittel" im Sinne der Richtlinie 95/46 dar.

74. Infolgedessen bin ich der Auffassung, dass die erste der vom Bundesgerichtshof vorgelegten Fragen, wie sie von ihm formuliert worden ist, zu bejahen ist. Die dynamische IP-Adresse ist für den Internetdiensteanbieter aufgrund der Existenz eines Dritten (des Internetzugangsanbieters), an den er sich vernünftigerweise wenden könnte, um andere zusätzliche Daten zu erhalten, die in Verbindung mit dieser IP-Adresse die Identifizierung eines Nutzers ermöglichen, als personenbezogenes Datum einzustufen.

75. Das Ergebnis, zu dem die gegenteilige Lösung führen würde, spricht für die von mir vorgeschlagene Antwort. Wenn dynamische IP-Adressen nicht als personenbezogene Daten für den Internetdiensteanbieter anzusehen wären, könnte dieser sie unbegrenzt speichern und jederzeit den Internetzugangsanbieter um die zusätzlichen Daten bitten, um sie mit der IP-Adresse zur Identifizierung des Nutzers zu verbinden. In diesem Fall würde, wie auch die deutsche Regierung

19 – Rn. 40 und 45 ihrer schriftlichen Erklärungen.

20 – In diesem Zusammenhang spielt es keine Rolle, dass der Zugang zu dem personenbezogenen Datum *de facto* durch eine Verletzung der Vorschriften über den Datenschutz möglich ist.

21 – Rn. 47 und 48 ihrer schriftlichen Erklärungen.

einräumt[22], aus einer dynamischen IP-Adresse ein personenbezogenes Datum, wenn er die geeigneten zusätzlichen Daten zur Identifizierung des Nutzers ohne Verstoß gegen Datenschutzbestimmungen bekommen hat.

76. Es würde sich dann um ein Datum handeln, dessen Speicherung nur deshalb möglich gewesen wäre, weil es bis zu diesem Zeitpunkt nicht als personenbezogenes Datum für den Internetdiensteanbieter angesehen worden wäre. Die rechtliche Qualifizierung der dynamischen IP-Adresse als personenbezogenes Datum läge damit in den Händen des Internetdiensteanbieters, da sie davon abhinge, dass dieser zu einem späteren Zeitpunkt beschlösse, die Adresse in Verbindung mit den zusätzlichen Daten, die er sich von einem Dritten verschaffen müsste, zur Identifizierung des Nutzers zu verwenden. Meines Erachtens ist jedoch nach dem Wortlaut der Richtlinie 95/46 entscheidend, dass – vernünftigerweise – von der Existenz eines „zugänglichen" Dritten ausgegangen werden kann, der über die erforderlichen Mittel verfügt, um die Identifizierung einer Person zu ermöglichen, und nicht, dass von der Möglichkeit, sich an diesen Dritten zu wenden, tatsächlich Gebrauch gemacht wird.

77. Man könnte mit der deutschen Regierung auch die Ansicht vertreten, dass die dynamische IP-Adresse sich erst in ein personenbezogenes Datum verwandelt, wenn der Internetzugangsanbieter sie erhält. Dann müsste man akzeptieren, dass diese Qualifizierung im Hinblick auf die Frist für die Speicherung der IP-Adresse rückwirkend erfolgt, und infolgedessen diese Adresse als inexistent ansehen, wenn der Zeitraum überschritten wurde, in dem sie hätte gespeichert werden können, wenn sie von Anfang an als ein personenbezogenes Datum eingestuft worden wäre. Damit käme man zu einem Ergebnis, dass dem Geist der Rechtsvorschriften über den Schutz personenbezogener Daten widerspräche. Der Grund dafür, dass eine Speicherung solcher Daten nur für einen begrenzten Zeitraum zulässig ist, würde verfälscht, wenn eine Eigenschaft, die diesen Daten von Anfang an innewohnt, möglicherweise mit Verspätung ihre Wirkung entfaltet: ihr Potenzial – allein oder in Verbindung mit anderen Daten –, der Identifizierung einer natürlichen Person zu dienen. Auch aus diesem rein praktischen Grund ist es sinnvoller, der IP-Adresse diese Eigenschaft von Anfang an zuzuerkennen.

78. Daher komme ich zu einem ersten Ergebnis, dem zufolge Art. 2 Buchst. a der Richtlinie 95/46 dahin auszulegen ist, dass eine IP-Adresse, die ein Diensteanbieter im Zusammenhang mit einem Zugriff auf seine Internetseite speichert, für diesen ein personenbezogenes Datum darstellt, soweit ein Internetzugangsanbieter über das zur Identifizierung der betroffenen Person erforderliche Zusatzwissen verfügt.

[22] – Rn. 36 ihrer schriftlichen Erklärungen.

B – *Zweite Frage*

79. Mit der zweiten Vorlagefrage möchte der Bundesgerichtshof wissen, ob Art. 7 Buchst. f der Richtlinie 95/46 einer nationalen Rechtsvorschrift entgegensteht, wonach personenbezogene Daten eines Nutzers ohne dessen Einwilligung nur erhoben und verwendet werden dürfen, soweit dies erforderlich ist, um die konkrete Inanspruchnahme des Telemediums durch diesen Nutzer zu ermöglichen und abzurechnen, wohingegen der Zweck, die Funktionsfähigkeit des Telemediums zu gewährleisten, die Verwendung dieser Daten nicht über das Ende des jeweiligen Nutzungsvorgangs hinaus rechtfertigen kann.

80. Vor einer Antwort hierauf bedarf es einer Klarstellung hinsichtlich der vom Bundesgerichtshof übermittelten Informationen, denen zufolge die streitgegenständlichen Daten gespeichert werden, um die Funktionsfähigkeit der im Ausgangsverfahren in Rede stehenden Internetseiten zu gewährleisten und gegen diese Seiten gerichtete Cyberangriffe gegebenenfalls strafrechtlich verfolgen zu können.

81. Es stellt sich daher vorab die Frage, ob die Verarbeitung der IP-Adressen, auf die sich das Vorabentscheidungsersuchen bezieht, unter die in Art. 3 Abs. 2 erster Gedankenstrich der Richtlinie 95/46 vorgesehene Ausnahme fällt[23].

1. Zur Anwendbarkeit der Richtlinie 95/46 auf die Verarbeitung der streitgegenständlichen Daten

82. Allem Anschein nach handelt die Bundesrepublik Deutschland im Ausgangsverfahren als reine Anbieterin von Internetdiensten, d. h. als Privatperson (und daher *sine imperio*). Daraus folgt, dass die Verarbeitung der hier streitgegenständlichen Daten grundsätzlich vom Anwendungsbereich der Richtlinie 95/46 nicht ausgeschlossen ist.

83. Mit den Worten des Gerichtshofs im Urteil Lindqvist[24] sind die in Art. 3 Abs. 2 erster Gedankenstrich der Richtlinie 95/46 aufgeführten Tätigkeiten „jedenfalls spezifische Tätigkeiten der Staaten oder der staatlichen Stellen und haben mit den Tätigkeitsbereichen von Einzelpersonen nichts zu tun“[25]. Soweit die Verarbeitung der streitgegenständlichen Daten durch einen Verantwortlichen erfolgt, der zwar eine staatliche Stelle ist, tatsächlich aber wie ein Privatrechtssubjekt handelt, findet die Richtlinie 95/46 Anwendung.

[23] – Nicht in den Anwendungsbereich der Richtlinie 95/46 fällt „die Verarbeitung [personenbezogener] Daten … betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates … und die *Tätigkeiten des Staates im strafrechtlichen Bereich*“ (Hervorhebung nur hier).

[24] – Urteil vom 6. November 2003 (C-101/01, EU:C:2003:596, Rn. 43).

[25] – Gleichlautend das Urteil vom 16. Dezember 2008, Satakunnan Markkinapörssi und Satamedia (C-73/07, EU:C:2008:727, Rn. 41).

84. Das vorlegende Gericht betont, dass der Hauptzweck, den die deutsche Verwaltung mit der Speicherung der dynamischen IP-Adressen verfolge, die „Gewährleistung und Aufrechterhaltung der Sicherheit und Funktionsfähigkeit ihrer Telemedien“ sei; insbesondere die Förderung der „Erkennung und Abwehr häufig auftretender ‚Denial-of-Service‘-Attacken, bei denen die TK-Infrastruktur durch gezieltes und koordiniertes Fluten einzelner Webserver mit einer Vielzahl von Anfragen lahm gelegt wird“[26]. Die Speicherung dynamischer IP-Adressen zu diesem Zweck kann für jeden Inhaber einer Internetseite gleichermaßen von einer gewissen Bedeutung sein und impliziert weder unmittelbar noch mittelbar die Ausübung öffentlicher Gewalt, weshalb die Richtlinie 95/46 ohne besondere Schwierigkeiten auf eine solche Speicherung Anwendung finden kann.

85. Der Bundesgerichtshof betont allerdings, dass die Speicherung der dynamischen IP-Adressen durch die im Ausgangsverfahren in Rede stehenden Diensteanbieter auch dazu diene, die Urheber möglicher Cyberangriffe gegebenenfalls strafrechtlich zu verfolgen. Reicht dieser Zweck aus, um die Verarbeitung dieser Daten vom Anwendungsbereich der Richtlinie 95/46 auszunehmen?

86. Meines Erachtens liegt, wenn mit „Strafverfolgung“ die Ausübung des *ius puniendi* des Staates durch die im Ausgangsverfahren beklagten Diensteanbieter zu verstehen ist, eine „Tätigkeit des Staates im strafrechtlichen Bereich“ vor und damit eine der in Art. 3 Abs. 2 erster Gedankenstrich der Richtlinie 95/46 vorgesehenen Ausnahmen.

87. In diesem Fall ist im Einklang mit der Rechtsprechung des Gerichtshofs in der Rechtssache Huber[27] die Verarbeitung personenbezogener Daten durch die Diensteanbieter im Interesse der Sicherheit und technischen Funktionsfähigkeit ihrer Telemedien vom Anwendungsbereich der Richtlinie 95/46 umfasst, während die Verarbeitung von Daten zum Zweck der Tätigkeit des Staates im strafrechtlichen Bereich nicht unter die Richtlinie fällt.

88. Ebenso würde, auch wenn die Bundesrepublik Deutschland in ihrer Eigenschaft als reine Diensteanbieterin ohne hoheitliche Befugnisse nicht zur Strafverfolgung im eigentlichen Sinne befugt ist und sich wie jede Privatperson darauf beschränkt, die streitgegenständlichen IP-Adressen einer staatlichen Stelle zum Zweck der Strafverfolgung zu übermitteln, die Verarbeitung der dynamischen IP-Adressen einen Zweck verfolgen, der nicht in den Anwendungsbereich der Richtlinie 95/46 fiele.

89. Dies ergibt sich aus der Rechtsprechung in der Rechtssache Parlament/Rat und Kommission[28], in der der Gerichtshof feststellte, dass die Tatsache, dass

[26] – Rn. 36 des Vorabentscheidungsersuchens.

[27] – Urteil vom 16. Dezember 2008 (C-524/06, EU:C:2008:724, Rn. 45).

[28] – Urteil vom 30. Mai 2006 (C-317/04 und C-318/04, EU:C:2006:346, Rn. 54 bis 59).

bestimmte personenbezogene Daten von „private[n] Wirtschaftsteilnehmer[n] … zu gewerblichen Zwecken erhoben … und in einen Drittstaat übermittel[t wurden]“, nicht bedeutet, dass diese Übermittlung „nicht in den Anwendungsbereich“ von Art. 3 Abs. 2 erster Gedankenstrich der Richtlinie 95/46 fällt, wenn der Zweck der Übermittlung Tätigkeiten des Staates im strafrechtlichen Bereich zum Gegenstand hat, sofern sie in dem fraglichen Fall „in einem von staatlichen Stellen geschaffenen Rahmen statt[findet] und … der öffentlichen Sicherheit [dient]“[29].

90. Wenn dagegen, wie sich meiner Meinung nach dem Vorlagebeschluss entnehmen lässt, mit „Strafverfolgung“ das Vorgehen einer Privatperson gemeint ist, die das Recht hat, den Staat zur Ausübung seines *ius puniendi* durch entsprechendes Handeln aufzufordern, dann kann man nicht annehmen, dass die Verarbeitung der dynamischen IP-Adressen Tätigkeiten des Staates im strafrechtlichen Bereich zum Gegenstand hat und vom Anwendungsbereich der Richtlinie 95/46 ausgenommen ist.

91. In Wirklichkeit dienen die Speicherung und Aufzeichnung dieser Daten dann als ein weiteres Beweismittel, mit dem der Inhaber der Internetseite vom Staat die Verfolgung eines rechtswidrigen Verhaltens auf Antrag verlangen kann. Es handelt sich um ein strafrechtliches Mittel zur Verteidigung von Rechten, die die Rechtsordnung dem Einzelnen zuerkennt (in diesem Fall einer öffentlichen Stelle, die privatrechtlich handelt). So betrachtet unterscheidet sich dieses Vorgehen nicht vom Handeln eines beliebigen anderen Internetdiensteanbieters, der im Einklang mit den in der Rechtsordnung vorgesehenen Strafverfolgungsverfahren staatlichen Schutz sucht.

92. Soweit die deutsche Verwaltung als Internetdiensteanbieterin ohne hoheitliche Befugnisse auftritt, worüber das vorlegende Gericht entscheiden muss, ist daher die von ihr vorgenommene Verarbeitung dynamischer IP-Adressen als personenbezogener Daten vom Anwendungsbereich der Richtlinie 95/46 umfasst.

2. Zur Beantwortung der Frage

93. § 15 Abs. 1 TMG berechtigt lediglich zur Erhebung und Verwendung der personenbezogenen Daten eines Nutzers, soweit dies erforderlich ist, um die konkrete Inanspruchnahme eines Telemediums zu ermöglichen und abzurechnen. Genauer gesagt darf der Diensteanbieter nur die sogenannten „Nutzungsdaten“ erheben und verwenden, d. h. die personenbezogenen Daten eines Nutzers, die erforderlich sind, um „die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen“. Diese Daten sind zu löschen, sobald der Nutzungsvorgang beendet

[29] – Ebd. (Rn. 59). Es ging um personenbezogene Daten, deren Verarbeitung für die Erbringung der Dienste, die die Geschäftstätigkeit der betreffenden privaten Betreiber (Fluggesellschaften) darstellte, nicht erforderlich waren, zu deren Weitergabe an die US-amerikanischen Behörden die Betreiber sich aber zum Zweck der Verhütung und Bekämpfung des Terrorismus verpflichtet sahen.

ist (also sobald die konkrete Inanspruchnahme des Telemediums abgeschlossen ist), es sei denn, sie müssen gemäß § 15 Abs. 4 TMG „zum Zwecke der Abrechnung“ aufbewahrt werden.

94. Ist die Verbindung beendet, schließt § 15 TMG es offensichtlich aus, die Nutzungsdaten aus anderen Gründen zu speichern, auch nicht zur Gewährleistung „der [generellen] Inanspruchnahme von Telemedien“. Da diese Vorschrift des TMG sich ausschließlich auf Abrechnungszwecke als Rechtfertigungsgrund für die Speicherung von Daten bezieht, könnte man sie so verstehen (wenngleich ihre endgültige Auslegung dem vorlegenden Gericht zukommt), dass sie verlangt, dass die Nutzungsdaten nur zur Ermöglichung einer konkreten Verbindung verwendet werden dürfen und nach deren Beendigung gelöscht werden müssen.

95. Art. 7 Buchst. f der Richtlinie 95/46[30] erlaubt die Verarbeitung personenbezogener Daten unter Bedingungen, die meiner Ansicht nach großzügiger (für den für die Verarbeitung Verantwortlichen) gefasst sind als die in § 15 TMG formulierten. Die deutsche Vorschrift kann in diesem Punkt als restriktiver als die unionsrechtliche bezeichnet werden, weil sie die Verwirklichung eines anderen berechtigten Interesses, das nicht mit der Abrechnung des Dienstes in Zusammenhang steht, grundsätzlich nicht vorsieht, obwohl die Bundesrepublik Deutschland als Internetdiensteanbieterin auch ein berechtigtes Interesse daran haben könnte, die Funktionsfähigkeit ihrer Internetseiten über jeden einzelnen Nutzungsvorgang hinaus zu gewährleisten[31].

96. Die Rechtsprechung des Gerichtshofs gemäß seinem Urteil ASNEF und FECEMD[32] liefert die Kriterien für die Beantwortung der zweiten Vorlagefrage. Der Gerichtshof stellte dort fest, dass sich aus dem Ziel der Richtlinie 95/46 „ergibt …, dass Art. 7 der Richtlinie 95/46 eine erschöpfende und abschließende Liste der Fälle vorsieht, in denen eine Verarbeitung personenbezogener Daten als rechtmäßig angesehen werden kann“[33]. Demnach „dürfen die Mitgliedstaaten weder neue Grundsätze in Bezug auf die Zulässigkeit der Verarbeitung personenbezogener Daten neben Art. 7 der Richtlinie 95/46 einführen, noch zusätzliche Bedingungen stellen, die die Tragweite eines der sechs in diesem Artikel vorgesehenen Grundsätze verändern würden“[34].

30 – In Nr. 17 wiedergegeben.

31 – Siehe Nr. 84. Die Inhaber der Internetseiten haben sicherlich ein berechtigtes Interesse daran, die vom vorlegenden Gericht erwähnten „Denial-of-Service“-Attacken, d. h. massive Angriffe, die gelegentlich koordiniert gegen einzelne Internetseiten erfolgen, um diese zu überlasten und lahm zu legen, zu verhindern und zu bekämpfen.

32 – Urteil vom 24. November 2011 (C-468/10 und C-469/10, EU:C:2011:777).

33 – Ebd. (Rn. 30).

34 – Ebd. (Rn. 32).

97. § 15 TMG stellt zwar keine zusätzliche Bedingung neben denen auf, die in Art. 7 der Richtlinie 95/46 für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten vorgesehen sind – wie es in den Rechtssachen ASNEF und FECEMD der Fall war[35] –, aber er schränkt, wenn man ihn so restriktiv wie das vorlegende Gericht auslegt, die Bedingung in Buchst. f der genannten Bestimmung inhaltlich ein: Wo sich der Unionsgesetzgeber allgemein auf die Verwirklichung eines „berechtigten Interesses [bezieht], das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden“, berücksichtigt § 15 TMG einzig und allein die Notwendigkeit, „die [konkrete] Inanspruchnahme eines Telemediums zu ermöglichen und abzurechnen“.

98. Ebenso wie in der Rechtssache ASNEF und FECEMD[36] verändert auch in dieser Sache eine nationale Maßnahme – sofern sie, wie gesagt, so restriktiv ausgelegt wird wie oben erläutert – die Tragweite eines Grundsatzes des Art. 7 der Richtlinie 95/46, statt die Vorschrift lediglich näher zu regeln, was das Einzige ist, bei dem die Behörden der einzelnen Mitgliedstaaten gemäß Art. 5 der Richtlinie 95/46 einen gewissen Gestaltungsspielraum haben.

99. Dieser Art. 5 sieht vor: „Die Mitgliedstaaten bestimmen nach Maßgabe dieses Kapitels[37] die Voraussetzungen näher, unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist.“ Nichtsdestotrotz dürfen, wie in den Rechtssachen ASNEF und FECEMD[38] festgestellt, „die Mitgliedstaaten nach [dieser Vorschrift] auch keine anderen Grundsätze in Bezug auf die Zulässigkeit der Verarbeitung personenbezogener Daten als die in Art. 7 dieser Richtlinie aufgezählten Grundsätze einführen und auch nicht durch zusätzliche Bedingungen die Tragweite der sechs in diesem Art. 7 vorgesehenen Grundsätze verändern“.

100. § 15 TMG verkleinert im Vergleich zu Art. 7 Buchst. f der Richtlinie 95/46 den Umfang des berechtigten Interesses, das die Verarbeitung von Daten rechtfertigen kann, erheblich und regelt dieses Interesse im Rahmen der in Art. 5 der Richtlinie vorgesehenen Ermächtigung nicht lediglich näher oder genauer. Er tut dies zudem kategorisch und absolut und lässt nicht zu, dass der Schutz und die Gewährleistung der generellen Inanspruchnahme des Telemediums gemäß Art. 7 Buchst. f der Richtlinie 95/46 gegen „das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person, die gemäß Artikel 1 Absatz 1 geschützt sind“, abgewogen werden können.

35 – In diesem Fall hatte der nationale Gesetzgeber Art. 7 Buchst. f der Richtlinie 95/46 um die Bedingung ergänzt, dass die zu verarbeitenden Daten in öffentlich zugänglichen Quellen enthalten sein mussten.

36 – Urteil vom 24. November 2011 (C-468/10 und C-469/10, EU:C:2011:777).

37 – Kapitel II („Allgemeine Bedingungen für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten“), das die Art. 5 bis 21 der Richtlinie 95/46 umfasst.

38 – Urteil vom 24. November 2011 (C-468/10 und C-469/10, EU:C:2011:777, Rn. 36).

101. Letztlich hat der deutsche Gesetzgeber ebenso wie in den Rechtssachen ASNEF und FECEMD[39] „das Ergebnis der Abwägung der einander gegenüberstehenden Rechte und Interessen [für bestimmte Arten personenbezogener Daten] abschließend [vorgeschrieben], ohne Raum für ein Ergebnis zu lassen, das aufgrund besonderer Umstände des Einzelfalls anders ausfällt“, so dass es sich „nicht mehr um eine nähere Bestimmung im Sinne [des] Art. 5 [der Richtlinie 95/46 handelt]“.

102. Unter diesen Umständen bin ich der Auffassung, dass der Bundesgerichtshof verpflichtet ist, die nationale Regelung im Einklang mit der Richtlinie 95/46 auszulegen, was bedeutet: a) Zu den Gründen, die eine Verarbeitung der sogenannten „Nutzungsdaten“ rechtfertigen können, kann auch das berechtigte Interesse des Anbieters von Telemedien gehören, die generelle Inanspruchnahme dieser Medien zu gewährleisten. b) Dieses Interesse des Diensteanbieters kann im Einzelfall gegen das Interesse oder die Grundrechte und Grundfreiheiten des Nutzers abgewogen werden, um zu klären, welches Interesse gemäß Art. 1 Abs. 1 der Richtlinie 95/46 zu schützen ist[40].

103. Zu der Art und Weise, wie diese Interessenabwägung in dem zur Vorabentscheidung vorgelegten Fall durchzuführen ist, ist meiner Ansicht nach nichts weiter zu sagen. Der Bundesgerichtshof hat hierzu keine Frage vorgelegt, sondern sich Gedanken über die Lösung einer dieser Abwägung vorausgehenden Frage gemacht, ob nämlich diese Abwägung durchgeführt werden kann.

104. Schließlich scheint mir auch der Hinweis überflüssig, dass das vorlegende Gericht etwaige Rechtsvorschriften berücksichtigen kann, die der Mitgliedstaat im Rahmen der Ermächtigung nach Art. 13 Abs. 1 Buchst. d der Richtlinie 95/46 erlassen hat und die die in Art. 6 vorgesehenen Pflichten und Rechte beschränken können, sofern dies notwendig ist, um – neben anderen Rechtsgütern – „die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten“ zu gewährleisten. Auch auf diesen Punkt nimmt das vorlegende Gericht keinen Bezug, obwohl ihm zweifellos bekannt ist, dass es diese beiden Artikel gibt.

105. Demzufolge schlage ich vor, die zweite Vorlagefrage dahin zu beantworten, dass Art. 7 Buchst. f der Richtlinie 95/46 der Auslegung einer Vorschrift des nationalen Rechts entgegensteht, wonach ein Diensteanbieter daran gehindert ist, personenbezogene Daten eines Nutzers ohne dessen Einwilligung

[39] – Urteil vom 24. November 2011 (C-468/10 und C-469/10, EU:C:2011:777, Rn. 47).

[40] – Im Sitzungsprotokoll wies der Vertreter von Herrn Breyer das Argument zurück, dass die Speicherung der dynamischen IP-Adressen zum Schutz der Funktionsfähigkeit der Internetdienste vor möglichen Angriffen erforderlich sei. Ich denke nicht, dass sich dieses Problem für alle Fälle abstrakt lösen lässt. Der Lösung muss vielmehr in jedem Einzelfall eine Gegenüberstellung des Interesses des Inhabers der Internetseite und der Rechte und Interessen der Nutzer vorausgehen.

über das Ende des jeweiligen Nutzungsvorgangs hinaus zu erheben und zu verarbeiten, um die Funktionsfähigkeit des Telemediums zu gewährleisten.

VI – Ergebnis

106. Nach alledem schlage ich dem Gerichtshof vor, auf die Vorlagefragen wie folgt zu antworten:

1. Gemäß Art. 2 Buchst. a der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ist eine dynamische IP-Adresse, über die ein Nutzer die Internetseite eines Telemedienanbieters aufgerufen hat, für Letzteren ein „personenbezogenes Datum“, soweit ein Internetzugangsanbieter über weitere zusätzlichen Daten verfügt, die in Verbindung mit der dynamischen IP-Adresse die Identifizierung des Nutzers ermöglichen.

2. Art. 7 Buchst. f der Richtlinie 95/46 ist dahin auszulegen, dass der Zweck, die Funktionsfähigkeit des Telemediums zu gewährleisten, grundsätzlich als ein berechtigtes Interesse anzusehen ist, dessen Verwirklichung die Verarbeitung dieses personenbezogenen Datums rechtfertigt, sofern ihm Vorrang gegenüber dem Interesse oder den Grundrechten der betroffenen Person zuerkannt worden ist. Eine nationale Rechtsvorschrift, die die Berücksichtigung dieses berechtigten Interesses nicht zulässt, ist mit dem genannten Artikel nicht vereinbar.