URTEIL DES GERICHTSHOFS (Zweite Kammer)

19. Oktober 2016(*)

„Vorlage zur Vorabentscheidung – Verarbeitung personenbezogener Daten – Richtlinie 95/46/EG – Art. 2 Buchst. a – Art. 7 Buchst. f – Begriff ‚personenbezogene Daten' – Internetprotokoll-Adressen – Speicherung durch einen Anbieter von Online-Mediendiensten – Nationale Regelung, die eine Berücksichtigung des berechtigten Interesses des für die Verarbeitung Verantwortlichen nicht zulässt"

In der Rechtssache C-582/14

betreffend ein Vorabentscheidungsersuchen nach Art. 267 AEUV, eingereicht vom Bundesgerichtshof (Deutschland) mit Entscheidung vom 28. Oktober 2014, beim Gerichtshof eingegangen am 17. Dezember 2014, in dem Verfahren

Patrick Breyer

gegen

Bundesrepublik Deutschland

erlässt

DER GERICHTSHOF (Zweite Kammer)

unter Mitwirkung des Kammerpräsidenten M. Ilešič, der Richterin A. Prechal, des Richters A. Rosas (Berichterstatter), der Richterin C. Toader und des Richters E. Jarašiūnas,

Generalanwalt: M. Campos Sánchez-Bordona,

Kanzler: V. Giacobbo-Peyronnel, Verwaltungsrätin,

aufgrund des schriftlichen Verfahrens und auf die mündliche Verhandlung vom 25. Februar 2016,

unter Berücksichtigung der Erklärungen

– von Herrn Breyer, vertreten durch Rechtsanwalt M. Starostik,

– der deutschen Regierung, vertreten durch A. Lippstreu und T. Henze als Bevollmächtigte,

– der österreichischen Regierung, vertreten durch G. Eberhard als Bevollmächtigten,

– der portugiesischen Regierung, vertreten durch L. Inez Fernandes und C. Vieira Guerra als Bevollmächtigte,

– der Europäischen Kommission, vertreten durch P. J. O. Van Nuffel, H. Krämer, P. Costa de Oliveira und J. Vondung als Bevollmächtigte,

nach Anhörung der Schlussanträge des Generalanwalts in der Sitzung vom 12. Mai 2016

folgendes

Urteil

1 Das Vorabentscheidungsersuchen betrifft die Auslegung von Art. 2 Buchst. a und Art. 7 Buchst. f 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 (ABl. 1995, L 281, S. 31).

2 Dieses Ersuchen ergeht im Rahmen eines Rechtsstreits zwischen Herrn Patrick Breyer und der Bundesrepublik Deutschland über die Aufzeichnung und Speicherung der Internetprotokoll-Adresse (im Folgenden: IP-Adresse) von Herrn Breyer während seines Zugriffs auf mehrere Websites von Einrichtungen des Bundes.

Rechtlicher Rahmen

Unionsrecht

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

„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 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.“

4 Art. 1 der Richtlinie lautet:

„(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.“

5 In Art. 2 der Richtlinie heißt es:

„Im Sinne dieser Richtlinie bezeichnet der Ausdruck

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' die 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;

…"

6 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;

…"

7 Art. 5 der Richtlinie bestimmt:

„Die Mitgliedstaaten bestimmen nach Maßgabe dieses Kapitels die Voraussetzungen näher, unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist."

8 Art. 7 der Richtlinie 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, überwie[g]en."

9 In Art. 13 Abs. 1 der Richtlinie 95/46 heißt es:

„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

…

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

…"

Deutsches Recht

10 § 12 des Telemediengesetzes vom 26. Februar 2007 (BGBl. 2007 I S. 179, im Folgenden: TMG) bestimmt:

„(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.

(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."

11 § 15 TMG sieht vor:

„(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. …"

12 Gemäß § 3 Abs. 1 des Bundesdatenschutzgesetzes vom 20. Dezember 1990 (BGBl. 1990 I S. 2954) sind „[p]ersonenbezogene Daten … Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)".

Ausgangsrechtsstreit und Vorlagefragen

13 Herr Breyer rief mehrere Websites von Einrichtungen des Bundes ab. Auf diesen allgemein zugänglichen Websites stellen die genannten Einrichtungen aktuelle Informationen bereit.

14 Um Angriffe abzuwehren und die strafrechtliche Verfolgung von Angreifern zu ermöglichen, werden bei den meisten dieser Websites alle Zugriffe in Protokolldateien festgehalten. Darin werden nach dem Abruf der Website der Name der abgerufenen Seite bzw. Datei, in Suchfelder eingegebene Begriffe, der Zeitpunkt des Abrufs, die übertragene Datenmenge, die Meldung, ob der Abruf erfolgreich war, und die IP-Adresse des zugreifenden Computers gespeichert.

15 IP-Adressen sind Ziffernfolgen, die mit dem Internet verbundenen Computern zugewiesen werden, um deren Kommunikation im Internet zu ermöglichen. Beim Abruf einer Website wird die IP-Adresse des abrufenden Computers an den Server übermittelt, auf dem die abgerufene Website gespeichert ist. Dies ist erforderlich, um die abgerufenen Daten an den richtigen Empfänger übertragen zu können.

16 Des Weiteren geht aus der Vorlageentscheidung und der dem Gerichtshof vorliegenden Akte hervor, dass Internetzugangsanbieter den Computern der Internetnutzer entweder eine „statische“ IP-Adresse zuweisen oder eine „dynamische“ IP-Adresse, d. h. eine IP-Adresse, die sich bei jeder neuen Internetverbindung ändert. Anders als statische IP-Adressen erlauben dynamische IP-Adressen es nicht, anhand allgemein zugänglicher Dateien eine Verbindung zwischen einem Computer und dem vom Internetzugangsanbieter verwendeten physischen Netzanschluss herzustellen.

17 Herr Breyer hat bei den deutschen Verwaltungsgerichten eine Klage erhoben, mit der er beantragt, der Bundesrepublik Deutschland zu untersagen, die IP-Adresse seines zugreifenden Hostsystems über das Ende des Zugriffs auf allgemein zugängliche Websites für Online-Mediendienste der Einrichtungen des Bundes hinaus zu speichern oder durch Dritte speichern zu lassen, soweit die Speicherung nicht im Störungsfall zur Wiederherstellung der Verfügbarkeit des Telemediums erforderlich ist.

18 Die Klage von Herrn Breyer wurde im ersten Rechtszug abgewiesen; dagegen hat er Berufung eingelegt.

19 Das Berufungsgericht hat die abweisende Entscheidung teilweise abgeändert. Es hat die Bundesrepublik Deutschland verurteilt, es zu unterlassen, die IP-Adresse des zugreifenden Hostsystems von Herrn Breyer, die im Zusammenhang mit seinem Zugriff auf allgemein zugängliche Websites für Online-Mediendienste der Einrichtungen des Bundes übertragen wird, über das Ende des jeweiligen Nutzungsvorgangs hinaus zu speichern oder durch Dritte speichern zu lassen, sofern diese Adresse in Verbindung mit dem Zeitpunkt des über sie vorgenommenen Zugriffs gespeichert wird und Herr Breyer während dieses Zugriffs seine Personalien, auch in Form einer die Personalien ausweisenden E-Mail-Anschrift, angegeben hat, soweit die Speicherung nicht im Störungsfall zur Wiederherstellung der Verfügbarkeit des Telemediums erforderlich ist.

20 Das Berufungsgericht hat ausgeführt, eine dynamische IP-Adresse sei in Verbindung mit dem Zeitpunkt des über sie vorgenommenen Zugriffs ein personenbezogenes Datum, sofern der Nutzer der Website während des Vorgangs seine Personalien angegeben habe, weil der Betreiber der Website den Nutzer dadurch ermitteln könne, dass er dessen Namen mit der IP-Adresse seines Computers verknüpfe.

21 Im Übrigen sei der Klage von Herrn Breyer jedoch nicht stattzugeben. Gebe Herr Breyer nämlich während eines Nutzungsvorgangs seine Personalien nicht an, könne nur der Internetzugangsanbieter die IP-Adresse einem bestimmten Anschlussinhaber zuordnen. In den Händen der Bundesrepublik Deutschland als Anbieter von Online-Mediendiensten sei die IP-Adresse hingegen – auch in Verbindung mit dem Zeitpunkt des über sie vorgenommenen Zugriffs – kein personenbezogenes Datum, weil der Nutzer der betreffenden Websites für diesen Mitgliedstaat nicht bestimmbar sei.

22 Gegen die Entscheidung des Berufungsgerichts haben sowohl Herr Breyer als auch die Bundesrepublik Deutschland Revision beim Bundesgerichtshof (Deutschland) eingelegt. Herr Breyer beantragt, seinem Antrag auf Untersagung in vollem Umfang stattzugeben. Die Bundesrepublik Deutschland beantragt, diesen Antrag zurückzuweisen.

23 Das vorlegende Gericht führt aus, die von der als Anbieter von Online-Mediendiensten handelnden Bundesrepublik Deutschland gespeicherten dynamischen IP-Adressen des Computers von Herrn Breyer seien zumindest im Kontext mit den weiteren in den Protokolldateien gespeicherten Daten als Einzelangaben über sachliche Verhältnisse von Herrn Breyer anzusehen, da sie Aufschluss darüber gäben, dass er zu bestimmten Zeitpunkten bestimmte Seiten bzw. Dateien über das Internet abgerufen habe.

24 Die so gespeicherten Daten ließen aber aus sich heraus keinen unmittelbaren Rückschluss auf die Identität von Herrn Breyer zu. Die Betreiber der im Ausgangsverfahren in Rede stehenden Websites könnten die Identität von Herrn Breyer nämlich nur dann bestimmen, wenn dessen Internetzugangsanbieter ihnen Informationen über die Identität dieses Nutzers übermittele. Für die Einstufung dieser Daten als „personenbezogen“ komme es daher darauf an, ob die Identität von Herrn Breyer bestimmbar gewesen sei.

25 In der Lehre bestehe eine Kontroverse hinsichtlich der Frage, ob für die Feststellung, ob eine Person bestimmbar sei, auf ein „objektives“ oder ein „relatives“ Kriterium abzustellen sei. Die Anwendung eines „objektiven“ Kriteriums hätte zur Folge, dass Daten wie die im Ausgangsverfahren in Rede stehenden IP-Adressen nach dem Abrufen der betreffenden Websites als personenbezogen angesehen werden könnten, selbst wenn ausschließlich ein Dritter in der Lage sei, die Identität des Betroffenen festzustellen. Dabei sei der Dritte im vorliegenden Fall der Internetzugangsanbieter von Herrn Breyer, der Zusatzdaten gespeichert habe, die die Identifizierung von Herrn Breyer anhand der IP-Adressen ermöglichten. Nach einem „relativen“ Kriterium könnten diese Daten für eine Stelle wie den Internetzugangsanbieter von Herrn Breyer als personenbezogen angesehen werden, da sie die genaue Identifizierung des Nutzers ermöglichten (vgl. insoweit Urteil vom 24. November 2011, Scarlet Extended, C-70/10, EU:C:2011:771, Rn. 51), während sie für eine andere Stelle wie den Betreiber der von Herrn Breyer abgerufenen Websites nicht personenbezogen seien, da dieser Betreiber, sofern Herr Breyer während des Abrufens dieser Websites keine Personalien angegeben habe, nicht über die Informationen verfüge, die erforderlich seien, um ihn ohne unverhältnismäßigen Aufwand zu identifizieren.

26 Für den Fall, dass die dynamischen IP-Adressen des Computers von Herrn Breyer in Verbindung mit dem Zeitpunkt des über sie vorgenommenen Zugriffs als personenbezogene Daten anzusehen sein sollten, möchte das vorlegende Gericht wissen, ob die Speicherung dieser IP-Adressen über den Zugriff hinaus gemäß Art. 7 Buchst. f der Richtlinie 95/46 zulässig ist.

27 Hierzu führt der Bundesgerichtshof zum einen aus, dass die Anbieter von Online-Mediendiensten nach § 15 Abs. 1 TMG personenbezogene Daten eines Nutzers nur erheben und verwenden dürften, soweit dies erforderlich sei, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen. Zum anderen sei nach Ansicht der Bundesrepublik Deutschland die Speicherung dieser Daten zur Gewährleistung und Aufrechterhaltung der Sicherheit und Funktionsfähigkeit der von ihr allgemein zugänglich gemachten Websites für Online-Mediendienste erforderlich, insbesondere um sogenannte „Denial-of-Service“-Cyberangriffe, mit denen die Funktionsfähigkeit dieser Websites durch gezieltes und koordiniertes Fluten einzelner Webserver mit einer Vielzahl von Anfragen lahm gelegt werden solle, zu erkennen und diese Angriffe zu bekämpfen.

28 Wenn und soweit Maßnahmen des Anbieters von Online-Mediendiensten erforderlich seien, um solche Angriffe abzuwehren, könnten sie als erforderlich angesehen werden, um im Sinne von § 15 TMG „die Inanspruchnahme von Telemedien zu ermöglichen“. In der Literatur werde allerdings überwiegend die Auffassung vertreten, dass die Erhebung und Verwendung personenbezogener Daten eines Nutzers einer Website nur erlaubt sei, um eine konkrete Nutzung der Website zu ermöglichen, und dass die Daten, soweit sie nicht für Abrechnungszwecke benötigt würden, mit dem Ende des jeweiligen Nutzungsvorgangs zu löschen seien. Ein solches enges Verständnis des § 15 Abs. 1 TMG würde einer Erlaubnis, die IP-Adressen zur generellen Gewährleistung und Aufrechterhaltung der Sicherheit und Funktionsfähigkeit von Telemedien zu speichern, entgegenstehen.

29 Es sei fraglich, ob die letztgenannte, vom Berufungsgericht befürwortete enge Auslegung mit Art. 7 Buchst. f der Richtlinie 95/46 im Einklang stehe, insbesondere in Anbetracht der vom Gerichtshof in den Rn. 29 ff. des Urteils vom 24. November 2011, ASNEF und FECEMD (C-468/10 und C-469/10, EU:C:2011:777), aufgestellten Kriterien.

30 Unter diesen Umständen hat der Bundesgerichtshof beschlossen, das Verfahren auszusetzen und dem Gerichtshof folgende Fragen zur Vorabentscheidung vorzulegen:

1. Ist Art. 2 Buchst. a der Richtlinie 95/46 dahin auszulegen, dass eine IP-Adresse, die ein Anbieter von Online-Mediendiensten 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 Richtlinie 95/46 einer Vorschrift des nationalen Rechts entgegen, wonach der Anbieter von Online-Mediendiensten 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?

Zu den Vorlagefragen

Zur ersten Frage

31 Mit seiner ersten Frage möchte das vorlegende Gericht wissen, ob Art. 2 Buchst. a der Richtlinie 95/46 dahin auszulegen ist, dass eine dynamische IP-Adresse, die von einem Anbieter von Online-Mediendiensten beim Zugriff einer Person auf eine Website, die dieser Anbieter allgemein zugänglich macht, gespeichert wird, für den Anbieter ein personenbezogenes Datum im Sinne der genannten Bestimmung darstellt, wenn nur ein Dritter – hier der Internetzugangsanbieter dieser Person – über die zu ihrer Identifizierung erforderlichen Zusatzinformationen verfügt.

32 Nach Art. 2 Buchst. a der Richtlinie 95/46 bezeichnet der Ausdruck „personenbezogene Daten“ „alle Informationen über eine bestimmte oder bestimmbare natürliche Person (‚betroffene Person‘)“. Weiter heißt es dort, dass eine Person als bestimmbar angesehen wird, 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.

33 Einleitend ist darauf hinzuweisen, dass der Gerichtshof in Rn. 51 des Urteils vom 24. November 2011, Scarlet Extended (C-70/10, EU:C:2011:771), das u. a. die Auslegung der Richtlinie 95/46 betraf, im Wesentlichen festgestellt hat, dass es sich bei IP-Adressen um geschützte personenbezogene Daten handelt, da sie die genaue Identifizierung der Nutzer ermöglichen.

34 Diese Feststellung des Gerichtshofs betraf jedoch einen Fall, in dem die Sammlung und Identifizierung der IP-Adressen der Internetnutzer von den Internetzugangsanbietern vorgenommen werden sollte.

35 Vorliegend betrifft die erste Frage jedoch den Fall, dass die Bundesrepublik Deutschland als Anbieter von Online-Mediendiensten die IP-Adressen der Nutzer einer von ihr allgemein zugänglich gemachten Website speichert, ohne über die zur Identifizierung dieser Nutzer erforderlichen Zusatzinformationen zu verfügen.

36 Zudem steht fest, dass die vom vorlegenden Gericht angesprochenen IP-Adressen „dynamische“ IP-Adressen sind, d. h. vorübergehende Adressen, die bei jeder Internetverbindung zugewiesen und bei späteren Verbindungen ersetzt werden, und keine „statischen“ IP-Adressen, die unveränderlich sind und die dauerhafte Identifizierung des an das Netz angeschlossenen Geräts ermöglichen.

37 Die erste Frage des vorlegenden Gerichts beruht somit auf der Prämisse, dass Daten, die aus einer dynamischen IP-Adresse und dem Zeitpunkt des über sie vorgenommenen Zugriffs auf eine Website bestehen und von einem Anbieter von Online-Mediendiensten gespeichert werden, für sich genommen diesem Anbieter nicht die Möglichkeit bieten, den Nutzer zu bestimmen, der die Website während dieses Zugriffs abgerufen hat, während der Internetzugangsanbieter über Zusatzinformationen verfügt, die – in Verbindung mit der IP-Adresse – eine Bestimmung des Nutzers ermöglichen würden.

38 Insoweit ist zunächst festzustellen, dass eine dynamische IP-Adresse unstreitig keine Information darstellt, die sich auf eine „bestimmte natürliche Person“ bezieht, da sich aus ihr unmittelbar weder die Identität der natürlichen Person ergibt, der der Computer gehört, von dem aus eine Website abgerufen wird, noch die Identität einer anderen Person, die diesen Computer benutzen könnte.

39 Um zu klären, ob eine dynamische IP-Adresse in dem in Rn. 37 des vorliegenden Urteils dargestellten Fall für einen Anbieter von Online-Mediendiensten ein personenbezogenes Datum im Sinne von Art. 2 Buchst. a der Richtlinie 95/46 darstellt, ist sodann zu prüfen, ob eine solche vom Anbieter gespeicherte IP-Adresse als Information über eine „bestimmbare natürliche Person“ eingestuft werden kann, wenn die zur Identifizierung des Nutzers einer Website, die der betreffende Diensteanbieter allgemein zugänglich macht, erforderlichen Zusatzinformationen dem Internetzugangsanbieter des Nutzers vorliegen.

40 Insoweit geht aus dem Wortlaut von Art. 2 Buchst. a der Richtlinie 95/46 hervor, dass nicht nur eine direkt identifizierbare, sondern auch eine indirekt identifizierbare Person als bestimmbar angesehen wird.

41 Die Verwendung des Begriffs „indirekt“ durch den Unionsgesetzgeber deutet darauf hin, dass es für die Einstufung einer Information als personenbezogenes Datum nicht erforderlich ist, dass die Information für sich genommen die Identifizierung der betreffenden Person ermöglicht.

42 Zudem heißt es im 26. Erwägungsgrund der Richtlinie 95/46, dass bei der Entscheidung, ob eine Person bestimmbar ist, alle Mittel berücksichtigt werden sollten, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen.

43 Da dieser Erwägungsgrund auf die Mittel Bezug nimmt, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem „Dritten“ eingesetzt werden könnten, ist sein Wortlaut ein Indiz dafür, dass es für die Einstufung eines Datums als „personenbezogenes Datum“ im Sinne von Art. 2 Buchst. a der Richtlinie 95/46 nicht erforderlich ist, dass sich alle zur Identifizierung der betreffenden Person erforderlichen Informationen in den Händen einer einzigen Person befinden.

44 Dass über die zur Identifizierung des Nutzers einer Website erforderlichen Zusatzinformationen nicht der Anbieter von Online-Mediendiensten verfügt, sondern der Internetzugangsanbieter dieses Nutzers, vermag daher nicht auszuschließen, dass die von einem Anbieter von Online-Mediendiensten gespeicherten dynamischen IP-Adressen für ihn personenbezogene Daten im Sinne von Art. 2 Buchst. a der Richtlinie 95/46 darstellen.

45 Zu prüfen ist jedoch, ob die Möglichkeit, eine dynamische IP-Adresse mit den Zusatzinformationen zu verknüpfen, über die der Internetzugangsanbieter verfügt, ein Mittel darstellt, das vernünftigerweise zur Bestimmung der betreffenden Person eingesetzt werden kann.

46 Wie der Generalanwalt in Nr. 68 seiner Schlussanträge im Wesentlichen ausgeführt hat, wäre dies nicht der Fall, wenn die Identifizierung der betreffenden Person gesetzlich verboten oder praktisch nicht durchführbar wäre, z. B. weil sie einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften erfordern würde, so dass das Risiko einer Identifizierung *de facto* vernachlässigbar erschiene.

47 Das vorlegende Gericht weist in seiner Vorlageentscheidung zwar darauf hin, dass das deutsche Recht es dem Internetzugangsanbieter nicht erlaube, dem Anbieter von Online-Mediendiensten die zur Identifizierung der betreffenden Person erforderlichen Zusatzinformationen direkt zu übermitteln, doch gibt es offenbar – vorbehaltlich der vom vorlegenden Gericht insoweit vorzunehmenden Prüfungen – für den Anbieter von Online-Mediendiensten rechtliche Möglichkeiten, die es ihm erlauben, sich insbesondere im Fall von Cyberattacken an die zuständige Behörde zu wenden, um die fraglichen Informationen vom Internetzugangsanbieter zu erlangen und die Strafverfolgung einzuleiten.

48 Der Anbieter von Online-Mediendiensten verfügt somit offenbar über Mittel, die vernünftigerweise eingesetzt werden könnten, um mit Hilfe Dritter, und zwar der zuständigen Behörde und dem Internetzugangsanbieter, die betreffende Person anhand der gespeicherten IP-Adressen bestimmen zu lassen.

49 Nach alledem ist auf die erste Frage zu antworten, dass Art. 2 Buchst. a der Richtlinie 95/46 dahin auszulegen ist, dass eine dynamische IP-Adresse, die von einem Anbieter von Online-Mediendiensten beim Zugriff einer Person auf eine Website, die dieser Anbieter allgemein zugänglich macht, gespeichert wird, für den Anbieter ein personenbezogenes Datum im Sinne der genannten Bestimmung darstellt, wenn er über rechtliche Mittel verfügt, die es ihm erlauben, die betreffende Person anhand der Zusatzinformationen, über die der Internetzugangsanbieter dieser Person verfügt, bestimmen zu lassen.

Zur zweiten Frage

50 Mit seiner zweiten Frage möchte das vorlegende Gericht wissen, ob Art. 7 Buchst. f der Richtlinie 95/46 dahin auszulegen ist, dass er einer Regelung eines Mitgliedstaats entgegensteht, nach der ein Anbieter von Online-Mediendiensten personenbezogene Daten eines Nutzers dieser Dienste ohne dessen Einwilligung nur erheben und verwenden darf, soweit ihre Erhebung und ihre Verwendung erforderlich sind, um die konkrete Inanspruchnahme der Dienste durch den betreffenden Nutzer zu ermöglichen und abzurechnen, ohne dass der Zweck, die generelle Funktionsfähigkeit der Dienste zu gewährleisten, die Verwendung der Daten über das Ende eines Nutzungsvorgangs hinaus rechtfertigen kann.

51 Vor der Beantwortung dieser Frage ist zu klären, ob die Verarbeitung der im Ausgangsverfahren in Rede stehenden personenbezogenen Daten, d. h der dynamischen IP-Adressen der Nutzer bestimmter Websites von Einrichtungen des Bundes, nicht vom Anwendungsbereich der Richtlinie 95/46 ausgenommen ist, weil deren Art. 3 Abs. 2 erster Gedankenstrich vorsieht, dass die Richtlinie u. a. auf eine die Tätigkeiten des Staates im strafrechtlichen Bereich betreffende Verarbeitung personenbezogener Daten keine Anwendung findet.

52 Insoweit ist darauf hinzuweisen, dass alle in der genannten Bestimmung als Beispiele aufgeführten Tätigkeiten spezifische Tätigkeiten des Staates oder staatlicher Stellen sind und mit den Tätigkeitsbereichen Einzelner nichts zu tun haben (vgl. Urteile vom 6. November 2003, Lindqvist, C-101/01, EU:C:2003:596, Rn. 43, und vom 16. Dezember 2008, Satakunnan Markkinapörssi und Satamedia, C-73/07, EU:C:2008:727, Rn. 41).

53 Im Ausgangsverfahren handeln die Einrichtungen des Bundes, die Online-Mediendienste anbieten und für die Verarbeitung der dynamischen IP-Adressen verantwortlich sind, aber wohl – vorbehaltlich der vom vorlegenden Gericht insoweit vorzunehmenden Prüfungen – ungeachtet ihres Status als Behörden als Einzelne und nicht im Rahmen der Tätigkeiten des Staates im strafrechtlichen Bereich.

54 Daher ist zu klären, ob eine Regelung eines Mitgliedstaats wie die im Ausgangsverfahren in Rede stehende mit Art. 7 Buchst. f der Richtlinie 95/46 vereinbar ist.

55 Hierzu ist darauf hinzuweisen, dass die im Ausgangsverfahren in Rede stehende nationale Regelung bei einer Auslegung in dem vom vorlegenden Gericht angesprochenen engen Sinne die Erhebung und Verwendung personenbezogener Daten eines Nutzers der Online-Mediendienste ohne dessen Einwilligung nur gestattet, soweit dies erforderlich ist, um die konkrete Inanspruchnahme des Dienstes durch den fraglichen Nutzer zu ermöglichen und abzurechnen, ohne dass der Zweck, die generelle Funktionsfähigkeit des Dienstes zu gewährleisten, die Verwendung der Daten über das Ende eines Nutzungsvorgangs hinaus rechtfertigen kann.

56 Nach Art. 7 Buchst. f der Richtlinie 95/46 ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn sie „erforderlich [ist] 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 [der Richtlinie] geschützt sind, überwie[g]en“.

57 Der Gerichtshof hat entschieden, 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, und dass die Mitgliedstaaten weder neue Grundsätze in Bezug auf die Zulässigkeit der Verarbeitung personenbezogener Daten neben diesem Artikel einführen noch zusätzliche Bedingungen stellen dürfen, die die Tragweite eines der sechs darin vorgesehenen

Grundsätze verändern würden (vgl. in diesem Sinne Urteil vom 24. November 2011, ASNEF und FECEMD, C-468/10 und C-469/10, EU:C:2011:777, Rn. 30 und 32).

58 Art. 5 der Richtlinie 95/46 erlaubt den Mitgliedstaaten zwar, nach Maßgabe ihres Kapitels II und damit ihres Art. 7 die Voraussetzungen näher zu bestimmen, unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist, doch kann von dem Ermessen, über das die Mitgliedstaaten nach Art. 5 verfügen, nur im Einklang mit dem von der Richtlinie verfolgten Ziel der Wahrung eines Gleichgewichts zwischen dem freien Verkehr personenbezogener Daten und dem Schutz der Privatsphäre Gebrauch gemacht werden. Die Mitgliedstaaten dürfen nach Art. 5 der Richtlinie in Bezug auf die Zulässigkeit der Verarbeitung personenbezogener Daten keine anderen als die in Art. 7 der Richtlinie aufgezählten Grundsätze einführen und auch nicht durch zusätzliche Bedingungen die Tragweite der sechs in Art. 7 vorgesehenen Grundsätze verändern (vgl. in diesem Sinne Urteil vom 24. November 2011, ASNEF und FECEMD, C-468/10 und C-469/10, EU:C:2011:777, Rn. 33, 34 und 36).

59 Im vorliegenden Fall hätte § 15 TMG, wenn er in der in Rn. 55 des vorliegenden Urteils angesprochenen engen Weise ausgelegt würde, eine geringere Tragweite als der in Art. 7 Buchst. f der Richtlinie 95/46 aufgestellte Grundsatz.

60 Während nämlich in Art. 7 Buchst. f der Richtlinie allgemein auf die „Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden“, Bezug genommen wird, würde § 15 TMG dem Diensteanbieter die Erhebung und Verwendung personenbezogener Daten eines Nutzers nur gestatten, soweit dies erforderlich ist, um die konkrete Inanspruchnahme elektronischer Medien zu ermöglichen und abzurechnen. § 15 TMG stünde daher einer zur Gewährleistung der Inanspruchnahme von Online-Mediendiensten dienenden Speicherung personenbezogener Daten über das Ende eines Zugriffs auf diese Dienste hinaus allgemein entgegen. Die Einrichtungen des Bundes, die Online-Mediendienste anbieten, könnten aber auch ein berechtigtes Interesse daran haben, die Aufrechterhaltung der Funktionsfähigkeit der von ihnen allgemein zugänglich gemachten Websites über ihre konkrete Nutzung hinaus zu gewährleisten.

61 Wie der Generalanwalt in den Nrn. 100 und 101 seiner Schlussanträge ausgeführt hat, beschränkt sich eine solche nationale Regelung nicht darauf, den in Art. 7 Buchst. f der Richtlinie 95/46 enthaltenen Begriff des berechtigten Interesses im Einklang mit Art. 5 der Richtlinie näher zu bestimmen.

62 Insoweit ist ferner darauf hinzuweisen, dass Art. 7 Buchst. f der Richtlinie 95/46 einen Mitgliedstaat daran hindert, kategorisch und ganz allgemein die Verarbeitung bestimmter Kategorien personenbezogener Daten auszuschließen, ohne Raum für eine Abwägung der im konkreten Einzelfall einander gegenüberstehenden Rechte und Interessen zu lassen. Ein Mitgliedstaat kann daher für diese Kategorien das Ergebnis der Abwägung der einander gegenüberstehenden Rechte und Interessen nicht abschließend vorschreiben, ohne Raum für ein Ergebnis zu lassen, das aufgrund besonderer Umstände des Einzelfalls anders ausfällt (vgl. in diesem Sinne Urteil vom 24. November 2011, ASNEF und FECEMD, C-468/10 und C-469/10, EU:C:2011:777, Rn. 47 und 48).

63 Eine Regelung wie die im Ausgangsverfahren in Rede stehende schränkt jedoch hinsichtlich der Verarbeitung personenbezogener Daten der Nutzer von Online-Mediendiensten die Tragweite des in Art. 7 Buchst. f der Richtlinie 95/46 vorgesehenen Grundsatzes ein, indem sie es ausschließt, dass der Zweck, die generelle Funktionsfähigkeit des Online-Mediendienstes zu gewährleisten, Gegenstand einer Abwägung mit dem Interesse oder den Grundrechten und Grundfreiheiten der Nutzer sein kann, die nach dieser Bestimmung gemäß Art. 1 Abs. 1 der Richtlinie geschützt sind.

64 Nach alledem ist auf die zweite Frage zu antworten, dass Art. 7 Buchst. f der Richtlinie 95/46 dahin auszulegen ist, dass er einer Regelung eines Mitgliedstaats entgegensteht, nach der ein Anbieter von Online-Mediendiensten personenbezogene Daten eines Nutzers dieser Dienste ohne dessen Einwilligung nur erheben und verwenden darf, soweit ihre Erhebung und ihre Verwendung erforderlich sind, um die konkrete Inanspruchnahme der Dienste durch den betreffenden Nutzer zu ermöglichen und abzurechnen, ohne dass der Zweck, die generelle Funktionsfähigkeit der Dienste zu gewährleisten, die Verwendung der Daten über das Ende eines Nutzungsvorgangs hinaus rechtfertigen kann.

Kosten

65 Für die Parteien des Ausgangsverfahrens ist das Verfahren ein Zwischenstreit in dem beim vorlegenden Gericht anhängigen Rechtsstreit; die Kostenentscheidung ist daher Sache dieses Gerichts. Die Auslagen anderer Beteiligter für die Abgabe von Erklärungen vor dem Gerichtshof sind nicht erstattungsfähig.

Aus diesen Gründen hat der Gerichtshof (Zweite Kammer) für Recht erkannt:

1. 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 dahin auszulegen, dass eine dynamische Internetprotokoll-Adresse, die von einem Anbieter von Online-Mediendiensten beim Zugriff einer Person auf eine Website, die dieser Anbieter allgemein zugänglich macht, gespeichert wird, für den Anbieter ein personenbezogenes Datum im Sinne der genannten Bestimmung darstellt, wenn er über rechtliche Mittel verfügt, die es ihm erlauben, die betreffende Person anhand der Zusatzinformationen, über die der Internetzugangsanbieter dieser Person verfügt, bestimmen zu lassen.

2. Art. 7 Buchst. f der Richtlinie 95/46 ist dahin auszulegen, dass er einer Regelung eines Mitgliedstaats entgegensteht, nach der ein Anbieter von Online-Mediendiensten personenbezogene Daten eines Nutzers dieser Dienste ohne dessen Einwilligung nur erheben und verwenden darf, soweit ihre Erhebung und ihre Verwendung erforderlich sind, um die konkrete Inanspruchnahme der Dienste durch den betreffenden Nutzer zu ermöglichen und abzurechnen, ohne dass der Zweck, die generelle Funktionsfähigkeit der Dienste zu gewährleisten, die Verwendung der Daten über das Ende eines Nutzungsvorgangs hinaus rechtfertigen kann.