

Schriftliche Erklärungen

Rechtssache C-582/14\*

**Schriftstück eingereicht von:**

Portugiesische Republik

**Übliche Bezeichnung der Rechtssache:**

Breyer

**Eingangsdatum:**

6. April 2015

---

MINISTERIUM FÜR AUSWÄRTIGE ANGELEGENHEITEN

Generaldirektion für Europäische Angelegenheiten

**GERICHTSHOF**

**DER EUROPÄISCHEN UNION**

**Rechtssache C-582/14**

**Breyer**

**ERKLÄRUNGEN**

**DER**

**PORTUGIESISCHEN REPUBLIK**

zum Vorabentscheidungsersuchen des *Bundesgerichtshofs* (Deutschland) über die Auslegung 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 [Or. 2]

\* Verfahrenssprache: Deutsch.

Lissabon, den 27. März 201[5]

An den Präsidenten und die Richter  
des Gerichtshofs der Europäischen Union

Die **portugiesische Regierung**, vertreten durch [REDACTED]  
[REDACTED] als Bevollmächtigte, legt nach Zustellung des  
Vorabentscheidungsersuchens des *Bundesgerichtshofs* (Deutschland) in der  
Rechtssache C-582/14 gemäß Art. 23 des Protokolls über die Satzung des  
Gerichtshofs ihre nachfolgenden Erklärungen mit folgender Begründung vor:

### I – Sachverhalt

1. Nach den übermittelten Akten geht es in der vorliegenden Rechtssache um die Revision gegen das Urteil, mit dem die Berufung gegen die Entscheidung über eine gegen die *Bundesrepublik Deutschland* (im Folgenden: Beklagte) gerichtete Unterlassungsklage teilweise zurückgewiesen worden war, mit der der Kläger, Dr. Patrick Breyer (im Folgenden: Kläger), begehrt hatte, die Beklagte zu verurteilen, es zu unterlassen, die IP-Adresse seines zugreifenden Hostsystems, die bei der Nutzung öffentlich zugänglicher Telemedien der Beklagten über das Internet übertragen wird, über das Ende des jeweiligen Nutzungsvorgangs hinaus zu speichern oder durch Dritte speichern zu lassen. Der Kläger hatte nämlich eine Unterlassungsklage gegen die Bundesrepublik Deutschland erhoben, weil deren [Or. 3] Einrichtungen Internetprotokoll-Adressen (im Folgenden: IP-Adressen) speicherten.

2. Nach der sich aus den Akten ergebenden Definition sind „*IP-Adressen ... Ziffernfolgen, die vernetzten Computern zugewiesen werden, um deren Kommunikation im Internet zu ermöglichen*“. Bei Kommunikation über das Internet wird die IP-Adresse des Computers, der eine Internetseite abrufen, somit an den Server übermittelt, auf dem die abgerufene Seite gespeichert ist, und mittels dieser Adresse werden die vom Empfänger abgerufenen Daten an diesen übertragen.

3. In der Akte heißt es ferner, dass auf den meisten Internetportalen der Einrichtungen des Bundes, die über dieses Medium aktuelle Informationen für die Öffentlichkeit bereitstellen, zur Abwehr bössartiger Angriffe und zur Ermöglichung der strafrechtlichen Verfolgung der dafür Verantwortlichen alle Zugriffe auf diese Portale in Protokolldateien aufgezeichnet und festgehalten werden.

4. In der Akte heißt es außerdem, dass über das Ende des jeweiligen Nutzungsvorgangs hinaus Aufzeichnungen gespeichert und aufbewahrt werden, die Folgendes enthalten:

*den Namen der abgerufenen Datei bzw. Seite, in Suchfelder eingegebene Begriffe, den Zeitpunkt des Abrufs, die übertragene Datenmenge, die Meldung, ob der Abruf erfolgreich war, und die IP-Adresse des zugreifenden Rechners.*

5. Die Unterlassungsklage wurde abgewiesen. Das zweitinstanzliche Gericht hat der vom Kläger eingelegten Berufung jedoch teilweise stattgegeben und die Beklagte verurteilt,

*es zu unterlassen, die IP-Adresse des zugreifenden Hostsystems des Klägers, die im Zusammenhang mit der Nutzung öffentlich zugänglicher Telemedien der Beklagten im Internet – mit Ausnahme eines Internetportals – übertragen wird, in Verbindung mit dem Zeitpunkt des jeweiligen Nutzungsvorgangs über das Ende des jeweiligen Nutzungsvorgangs hinaus zu speichern oder durch Dritte speichern zu lassen, [Or. 4] sofern der Kläger während eines Nutzungsvorgangs seine Personalien, auch in Form einer die Personalien ausweisenden E-Mail-Anschrift, angibt und soweit die Speicherung nicht im Störungsfall zur Wiederherstellung der Verfügbarkeit des Telemediums erforderlich ist.*

6. Die Parteien legten gegen dieses Urteil Revision ein. Der Kläger begehrt die Verurteilung der Beklagten ohne die vorstehend genannten Beschränkungen. Die Beklagte verfolgt ihren Antrag auf vollständige Klageabweisung weiter. Hinsichtlich des weiteren Sachverhalts wird auf die Akte verwiesen.

## **II – Fragen des vorlegenden Gerichts**

7. Das vorlegende Gericht hält für die Entscheidung über die Revision gegen das Urteil, mit dem der Berufung gegen die die Unterlassungsklage abweisende Entscheidung teilweise stattgegeben worden war, eine Vorabentscheidung des Gerichtshofs über folgende Fragen für erforderlich:

*1. Ist 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 – Datenschutz-Richtlinie – 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? [Or. 5]*

### III – Rechtliche Würdigung

#### a) Zur ersten Frage

8. Vorab ist darauf hinzuweisen, dass die 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 (im Folgenden: Datenschutzrichtlinie oder Richtlinie) in Art. 2 Buchst. a insofern eine recht weit gefasste Definition des Begriffs „personenbezogene Daten“ enthält, als dieser Folgendes erfasst: *„alle Informationen über eine bestimmte oder bestimmbare natürliche Person ...; als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer ...“*. Abgesehen von den Fällen, in denen eine Person sofort identifiziert werden kann, gibt es somit eine Reihe von möglichen Fällen, in denen eine nicht sofort identifizierte Person zu einem späteren Zeitpunkt identifiziert werden kann. Es kann sich dabei um eine direkte oder eine indirekte Identifizierbarkeit handeln, und die Identifizierung kann z. B. über die Entschlüsselung einer einzigen Person zugeordneten Nummer oder über die Verknüpfung verschiedener Informationen erfolgen.

9. Allein, dass eine Person anhand einer Information, wenn auch nur indirekt, identifiziert werden kann, eröffnet somit die Möglichkeit, diese Information als „personenbezogenes Datum“ einzustufen. „Personenbezogen“ sind die Daten jedoch nur, wenn die Person tatsächlich identifizierbar ist. Diese Beurteilung ist jeweils im Einzelfall auf der Grundlage der im Hinblick auf die Identifizierbarkeit vorliegenden konkreten Umstände vorzunehmen.

10. Im 26. Erwägungsgrund der Datenschutzrichtlinie werden die Kriterien genannt, die für die Beurteilung ausschlaggebend sind, ob ein oder mehrere Daten die Identifizierung einer Person ermöglichen: *„alle Mittel ..., die vernünftigerweise entweder [Or. 6] von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten ...“*. Dieser Beurteilungsmaßstab ist eindeutig dynamisch, da er die technologische Entwicklung, die eventuell mit der Identifizierung verbundenen Kosten, die Kapazitäten und die Natur des Nutzers der Daten und, stets je nach zu beurteilendem tatsächlich vorliegendem Fall, den beabsichtigten Zweck und die auf dem Spiel stehenden Interessen berücksichtigt<sup>1</sup>.

<sup>1</sup> Vgl. Stellungnahme 4/2007 der Datenschutzgruppe der EU (Artikel-29-Datenschutzgruppe) vom 20. Juni 2007 zum Begriff „personenbezogene Daten“ (WP 136). Siehe Anhang 1.

11. Der Einstufung der Daten als personenbezogene Daten kommt insofern besondere Bedeutung zu, als die Verarbeitung dieser Daten, wenn festgestellt wird, dass die Person anhand der Information bestimmbar ist, der gesetzlichen Datenschutzregelung unterliegt und unter Beachtung der entsprechenden für die Inhaber der Daten bestehenden Rechte und Garantien erfolgen muss.
12. Um eine (dynamische) IP-Adresse als „personenbezogenes Datum“ einzustufen zu können, ist zunächst zu prüfen, ob eine Person, hier in ihrer Eigenschaft als Nutzer, anhand dieser Adresse identifiziert werden kann und ob diese Identifizierung durch Mittel erreicht werden kann, die von dem für die Verarbeitung Verantwortlichen oder Dritten genutzt werden können.
13. Eine IP-Adresse dient der Identifizierung einer Internet-Verbindung und wird von den Zugangsanbietern systematisch zusammen mit dem Datum, dem Zeitpunkt, der Verbindungsdauer sowie den Daten des Nutzers/Internet-Teilnehmers in einem Protokoll festgehalten. Solange ein solches Protokoll mit der IP-Adresse eines Nutzers verknüpft werden kann, muss diese als personenbezogenes Datum betrachtet werden<sup>2</sup>. Das Unternehmen, das den Internetzugang anbietet, kann den fraglichen Nutzer folglich ohne große Schwierigkeiten identifizieren und muss hierfür keine besonderen Ermittlungen durchführen.
14. Im vorliegenden Fall hat die Behörde, die Dienstleistungen über ein Internet-Portal erbringt, auch die Möglichkeit, den Nutzer direkt zu identifizieren, [Or. 7] indem sie die IP-Adresse mit der Gesamtheit der zusätzlichen personenbezogenen Daten verknüpft, die übermittelt und anschließend verarbeitet werden. Doch selbst in den Fällen, in denen keine weiteren personenbezogenen Informationen erhoben werden, anhand deren die Beklagte den Inhaber der Daten direkt bestimmen könnte, muss davon ausgegangen werden, dass die IP-Adresse – die aufgezeichnet wird – in diesem Zusammenhang als „personenbezogenes Datum“ einzustufen ist, da sie, wie vorstehend ausgeführt, die Bestimmung des Nutzers durch einen Dritten ermöglicht.
15. Tatsächlich spielt es – so auch der Wortlaut des 26. Erwägungsgrundes der Datenschutzrichtlinie – keine Rolle, ob die für eine Identifizierung erforderlichen Schritte vom Verantwortlichen für die Verarbeitung oder „von einem Dritten“ vorgenommen werden. Diese Unterscheidung ist hier für die Feststellung, ob eine Person bestimmbar ist und ob die mit dieser verbundenen Daten somit als „personenbezogene Daten“ angesehen werden können, irrelevant.
16. In diesem Zusammenhang darf jedoch auch das Ziel nicht außer Acht gelassen werden, das der für die Verarbeitung Verantwortliche mit der Aufzeichnung und Speicherung der IP-Adressen der auf sein Internet-Portal zugreifenden Nutzer verfolgt. Die Beklagte führt aus, dass sie Angriffe abwehren

<sup>2</sup> Vgl. Arbeitsdokument der Datenschutzgruppe der EU (Artikel-29-Datenschutzgruppe) vom 21. November 2000 zur „Privatsphäre im Internet“ (WP 37). Siehe Anhang 2.

und Angreifer strafrechtlich verfolgen wolle. Das Aufzeichnen der IP-Adressen stellt jedoch an sich keine Maßnahme dar, mit der sich Angriffe verhindern lassen, sondern kann als vorbeugende Maßnahme angesehen werden, wenn man davon ausgeht, dass sich potenzielle Angreifer von Angriffen abhalten lassen, gerade weil die Möglichkeit besteht, sie zu identifizieren und entsprechend strafrechtlich zu verfolgen.

17. Zur Erreichung des angeführten Ziels der strafrechtlichen Verfolgung von Angreifern ist das Aufzeichnen der IP-Adresse jedoch unerlässlich, da es das einzige Mittel ist, das eine Identifizierung dieser Personen ermöglicht, wobei klar ist, dass diese Identifizierung durch Dritte erfolgt. Es wäre somit offensichtlich widersprüchlich, zu behaupten, dass es sich nicht um personenbezogene Daten handelt [Or. 8], weil die Personen nicht bestimmbar sind, wenn das Ziel der Verarbeitung dieser Daten gerade darin besteht, diese Personen zu bestimmen.

#### **b) Zur zweiten Frage**

18. Die in den Akten genannten §§ 12 und 15 des deutschen Telemediengesetzes (im Folgenden: TMG) sind eng an die Bestimmungen der Richtlinie 2002/58/EG<sup>3</sup> (bekannt als E-Privacy-Richtlinie) über Verkehrsdaten (Art. 6) angelehnt; zu dieser Datenkategorie gehören auch IP-Adressen<sup>4</sup>. Die bei der Verarbeitung von Verkehrsdaten geltenden Beschränkungen sind im deutschen Recht nämlich dieselben wie in der Richtlinie, insbesondere können diese Daten nicht ohne Einwilligung des Dateninhabers für andere Zwecke als den der Übertragung einer Nachricht oder der Gebührenabrechnung verwendet werden.

19. Diese restriktive Regelung der Richtlinie ist darauf zurückzuführen, dass es sich bei Verkehrsdaten wegen der Fülle der darin enthaltenen personenbezogenen Informationen, die Gewohnheiten, Verhaltensweisen und Freundeskreise<sup>5</sup> erkennen lassen, um besonders sensible Daten handelt, die daher einen erhöhten Schutz verdienen. In der vorliegenden Rechtssache liegt der Fall jedoch anders; der für die Verarbeitung Verantwortliche ist nämlich, da er kein Anbieter elektronischer Kommunikationsdienste im Sinne von Art. 3 Abs. 1 der Richtlinie [2002/58/EG] ist, nicht im Besitz aller Informationen, über die ein Telekommunikationsunternehmen verfügt.

20. Der deutsche Gesetzgeber hat sich jedoch dafür entschieden, für bestimmte Verarbeitungen von personenbezogenen Daten in besonderen Fällen eine strenge Schutzregelung vorzusehen, indem er die Verarbeitung von Verkehrsdaten – und damit die Nutzung von IP-Adressen – nur dann zulässt, wenn dies der Verfolgung

<sup>3</sup> Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (ABl. L 201 vom 31.7.2002, S. 37).

<sup>4</sup> Vgl. Art. 2 Buchst. b der Richtlinie 2002/58/EG.

<sup>5</sup> Vgl. Urteil des Gerichtshofs vom 8. April 2014 (C-[293/12] und C-594/12).

eines gesetzlich vorgesehenen Zwecks dient oder eine Einwilligung des Dateninhabers vorliegt. **[Or. 9]**

21. Nach der Datenschutzrichtlinie darf die Verarbeitung personenbezogener Daten nur dann erfolgen, wenn sie durch eine der in Art. 7 dieser Richtlinie genannten Rechtsgrundlagen legitimiert ist. Die Regelung in Art. 7 Buchst. f der Datenschutzrichtlinie – Verwirklichung des berechtigten Interesses des Verantwortlichen, sofern keine Rechte der Inhaber überwiegen – stellt eine Rechtsgrundlage für eine zulässige Verarbeitung von personenbezogenen Daten dar, wenn keine andere Grundlage gegeben ist. Ihre Anwendung ist immer auf den Einzelfall bezogen, da sie eine Ermessensentscheidung impliziert, eine Abwägung von Werten im konkreten Fall. Es geht hier jedoch nicht um die Umsetzung dieser Bestimmung in innerstaatliches deutsches Recht.

22. Im vorliegenden Fall gibt es ein nationales Gesetz, das die konkreten Bedingungen festlegt, unter denen die Verarbeitung von Daten zu bestimmten spezifischen Zwecken zu erfolgen hat. Es handelt sich hier um ein Spezialgesetz, das besondere Aspekte eines Tätigkeitsbereichs regelt, weshalb davon ausgegangen wird, dass die Abwägung zwischen den berechtigten Interessen des für die Verarbeitung Verantwortlichen und den Rechten und Freiheiten der Dateninhaber bereits vom Gesetzgeber vorgenommen wurde.

23. Eine andere Frage ist die nach der Auslegung von § 15 Abs. 1 TMG über die Zulässigkeit der Verarbeitung der IP-Adresse, um „die Inanspruchnahme von Telemedien“ zu ermöglichen, soweit diese Verarbeitung erforderlich ist, um die Sicherheit und die<sup>††</sup> Telemedien zu gewährleisten, womit sie unter eines der Ziele des Gesetzesbestimmung fällt. Bei dieser Frage ginge es um die Auslegung einer Vorschrift des deutschen Rechts und nicht des Unionsrechts.

24. Ob die Speicherung von IP-Adressen im Licht von § 15 Abs. 1 TMG für zulässig oder unzulässig erachtet wird, spielt nämlich keine Rolle für die Möglichkeit einer solchen Speicherung in Verwirklichung des berechtigten Interesses des Verantwortlichen nach Art. 7 Buchst. f der Datenschutzrichtlinie, sondern nur im Hinblick darauf, ob diese Option von der Gesetzesvorschrift umfasst ist. **[Or. 10]**

25. Es wird davon ausgegangen, dass Art. 7 Buchst. f der Datenschutzrichtlinie, gerade weil es sich dabei um eine Bestimmung handelt, die eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten bietet, wenn keine Einwilligung oder ein dazu ermächtigendes Gesetz vorliegen, nicht als Referenz bei der Auslegung nationaler Gesetze herangezogen werden kann, die ja bereits das Ergebnis einer Abwägung der betroffenen Interessen sind.

<sup>††</sup> Anm. d. Ü.: Hier fehlt offenbar ein Satzteil, evtl. „Funktionsfähigkeit der“ oder „Verfügbarkeit der“.

26. Zusammengefasst wird davon ausgegangen, dass Art. 7 Buchst. f der Datenschutzrichtlinie den fraglichen Vorschriften des nationalen deutschen Rechts bei der von der herrschenden Lehre vertretenen sogenannten engen Auslegung nicht entgegensteht.

#### IV – Ergebnis

27. Angesichts des Vorstehenden und aus den dargelegten Gründen schlägt die portugiesische Regierung dem Gerichtshof vor, die vom *Bundesgerichtshof* (Deutschland) vorgelegten Fragen in folgendem Sinne zu beantworten:

*Die 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 und insbesondere deren Art. 2 Buchst. a und 7 Buchst. f sind dahin auszulegen, dass*

*- eine Internetprotokoll-Adresse, die ein Diensteanbieter im Zusammenhang mit einem Zugriff auf seine Internetseite wie dem im Ausgangsverfahren in Rede stehenden speichert, für diesen schon dann ein personenbezogenes Datum darstellt, wenn ein Dritter, d. h. der Zugangsanbieter, über das zur Identifizierung der betroffenen Person erforderliche Zusatzwissen verfügt;*

*- sie einer Vorschrift des nationalen Rechts wie der im Ausgangsverfahren in Rede stehenden nicht entgegenstehen, wonach der Diensteanbieter personenbezogene Daten eines Nutzers ohne dessen Einwilligung [Or. 11] 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.*

Die Bevollmächtigten der Portugiesischen Republik

... [nicht übersetzt; Vermerk über die elektronische Signatur] [Or. 12]

Liste der Anhänge in der Rechtssache C-582/14 – Breyer

Anhang 1 – Stellungnahme 4/2007 der Datenschutzgruppe der EU (Artikel-29-Datenschutzgruppe) vom 20. Juni 2007 zum Begriff „personenbezogene Daten“ (WP 136).

Anhang 2 – Arbeitsdokument der Datenschutzgruppe der EU (Artikel-29-Datenschutzgruppe) vom 21. November 2000 zur „Privatsphäre im Internet“ (WP 37).