Bundesrepublik Deutschland

Berlin, den 2. April 2015

[redacted]
Bevollmächtigte der Regierung
der Bundesrepublik Deutschland

Gerichtshof der Europäischen Union
– Kanzlei –
2925 Luxemburg

Per e-Curia

ZUSTELLUNGEN
Bevorzugt per e-Curia oder an:
Bundesministerium für
Wirtschaft und Energie
Referat EA5
Scharnhorststr. 34 - 37
10115 Berlin
Deutschland
Telefax: +49 30 18615 - 5334

Stellungnahme

In der Rechtssache C-582/14

betreffend das dem Gerichtshof der Europäischen Union vom Bundesgerichtshof mit Beschluss vom 28. Oktober 2014 vorgelegte Vorabentscheidungsersuchen in dem dort anhängigen Rechtsstreit

Dr. Patrick Breyer

gegen

Bundesrepublik Deutschland

nehmen wir namens und in Vollmacht der Regierung der Bundesrepublik Deutschland wie folgt Stellung:

Inhaltsverzeichnis

A. EINLEITUNG

1 Das Vorabentscheidungsersuchen betrifft die Auslegung von Art. 2 Buchstabe a und Artikel 7 Buchstabe 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[1] (sog. Datenschutz-Richtlinie).

2 Das Ersuchen ergeht im Rahmen eines Rechtsstreits zwischen Dr. Patrick Breyer und der Bundesrepublik Deutschland wegen der Speicherung von dynamischen Internetprotokoll-Adressen (im Folgenden: IP-Adressen).

B. RECHTLICHER RAHMEN

Unionsrecht

Richtlinie 95/46

3 In den Erwägungsgründen der Richtlinie 95/46 heißt es auszugsweise 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 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. 2 der Richtlinie 95/46 bestimmt auszugsweise:

> „Begriffsbestimmungen
>
> 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;"

---

[1] ABl. EG 1995, L 281, S. 31.

C. SACHVERHALT UND VORLAGEFRAGEN

5 Der Kläger wandte sich im Wege einer zivilrechtlichen Unterlassungsklage gegen die Bundesrepublik Deutschland als Beklagte, um ihr die Speicherung der ihm bei seinen Zugriffen auf die Telemedienangebote der Beklagten jeweils zugewiesenen (dynamischen) IP-Adressen untersagen zu lassen. Die Organe und Behörden der Bundesrepublik Deutschland unterhalten zahlreiche, ans Internet angeschlossene Rechner (Server), auf denen sie Informationsangebote (Inhalte) zum Abruf durch jedermann vorhalten. Zum Teil werden staatliche Inhalte auch auf den Servern privater Betreiber zum Abruf vorgehalten (gehostet).

6 Bei vielen dieser von der Bundesrepublik Deutschland selbst oder von den privaten Betreibern vorgehaltenen Servern werden die IP-Adressen zugreifender Internetnutzer protokolliert und über das Ende des Nutzungsvorgangs hinaus vorgehalten, um Angriffe, insbesondere sog. „Denial of Service"-Attacken, erkennen und abwehren und die strafrechtliche Verfolgung von Angreifern durch Polizei und Justiz veranlassen zu können. Der Betrieb von Hardware und Inhalteangebot soll auch im Fall von Attacken aus dem Internet aufrechterhalten werden. Außerdem sollen nachträglich Fälle von Hacking und Computersabotage nachvollzogen werden können, die in der Vergangenheit begonnen haben, seinerzeit nicht erkannt wurden und erst mit Eintritt eines Schadens oder einer Betriebsunterbrechung aufgefallen sind.

7 IP-Adressen sind eindeutige, im Internet nur einmal vorkommende Kennziffern, die es Internetnutzern ermöglichen, im Internet eingestellte Inhalte an sich übertragen zu lassen, d.h. abzurufen. Gegenstand des Ausgangsverfahrens sind dynamische IP-Adressen. Diese sind als Nummernkontingente Internetzugangsanbietern (Internet Access Provider) wie beispielsweise Telekom, Vodafone oder Arcor zugeordnet und werden den Vertragskunden während deren Internetnutzung temporär zur Verfügung gestellt (von wenigen Sekunden bis maximal 24 Stunden, spätestens dann erfolgt eine Neuvergabe).

8 Anders als der Internetzugangsanbieter können Serverbetreiber und Inhalteanbieter (= Internet Service Provider im Gegensatz zu Internet Access Providern), die die IP-Nummern zugreifender Internetnutzer speichern, anhand dieser IP-Adressen – zusammen mit Tag und Zeit der Nutzung – nicht den Bezug zu dem Nutzer, dem die IP-Nummer zum fraglichen Tag und Zeitpunkt zur Nutzung überlassen worden war, herstellen.

9 Der Kläger des Ausgangsverfahrens bestreitet die Berechtigung von Serverbetreibern und Inhalteanbietern, die dynamischen IP-Adressen zugreifender Internetnutzer zu protokollieren und zu speichern und vertritt die Ansicht, dass es sich dabei um personenbezogene Daten handle und keine Rechtsgrundlage für die Speicherung dieser Daten bestehe.

10 Die Beklagte ist hingegen der Auffassung, dass es sich bei dynamischen IP-Adressen in der vorliegenden Konstellation für Serverbetreiber und Inhalteanbieter nicht um personenbezogene Daten handle und sie diese Daten auch ohne eine gesetzliche Grundlage oder eine Einwilligung der Betroffenen speichern dürfe.

11 Vor diesem Hintergrund hat der Bundesgerichtshof dem Gerichtshof folgende Fragen zur Vorabentscheidung vorgelegt:

> 1. Ist Art. 2 Buchstabe 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 (ABl. EG 1995, L 281/31) – 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 Buchstabe 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?

12 Hinsichtlich der weiteren Einzelheiten verweist die Bundesregierung auf den Vorlagebeschluss des Bundesgerichtshofs vom 28. Oktober 2014.

D. RECHTLICHE WÜRDIGUNG

I. Zur ersten Vorlagefrage: IP-Adressen, die ein Diensteanbieter speichert, sind für diesen keine personenbezogenen Daten

13 Mit der ersten Vorlagefrage möchte der Bundesgerichtshof wissen, ob IP-Adressen, die ein Diensteanbieter im Zusammenhang mit einem Zugriff auf seine Internetseite speichert, für diesen schon dann personenbezogene Daten im Sinne von Art. 2 Buchstabe a der Richtlinie 95/46 darstellen, wenn ein Dritter (hier: Zugangsanbieter) über das zur Identifizierung der betroffenen Person erforderliche Zusatzwissen verfügt.

14 Zunächst ist klarzustellen, dass sich der Ausgangsfall und die Vorlagefrage des Bundesgerichtshofs auf die Verwendung **dynamischer IP-Adressen** beziehen und insbesondere nicht den Fall der statischen IP-Adressen umfassen. Außerdem betreffen Ausgangsfall und Vorlagefrage keine Konstellationen, in denen der Diensteanbieter Zusatzinformationen über den Internetnutzer durch Techniken wie z. B. das Setzen von Cookies, Web-Tracking oder Browser-Fingerabdruck hat oder erlangt. Die Bundesregierung wird in ihrer Stellungnahme auf die hier nicht relevanten Fälle nicht eingehen, sondern sich auf die entscheidungserhebliche Konstellation beschränken, dass allein ein Dritter (hier: Zugangsanbieter) über das zur Identifizierung der betroffenen Person erforderliche Zusatzwissen verfügt.

15 Im Ergebnis ist die Bundesregierung der Auffassung, dass die erste Vorlagefrage zu **verneinen** ist: Dynamische IP-Adressen stellen für einen Diensteanbieter (Serverbetreiber oder Inhalteanbieter) in einer Konstellation wie der des Ausgangsverfahrens keine personenbezogenen Daten dar. Dementsprechend handelt es sich auch bei den dynamischen IP-Adressen der auf Telemedien der Bundesrepublik Deutschland als Beklagte des Vorlageverfahrens zugreifenden Nutzer für die Bundesrepublik Deutschland als Diensteanbieter der Telemedien nicht um personenbezogene Daten.

16 Im Einzelnen: Die erste Vorlagefrage ist in zwei Schritten zu beantworten: Zunächst stellt sich die grundsätzliche Frage, nach welchen Maßstäben zu beurteilen ist, ob es sich um personenbezogene Daten im Sinne des Art. 2 Buchstabe a der Richtlinie handelt (1.). Unter Zugrundelegung dieser Maßstäbe ist dann eine Einordnung von dynamischen IP-Adressen in einer Konstellation wie der vorliegenden vorzunehmen (2.).

1. Das Merkmal der „Bestimmbarkeit" ist nach einem relativen Ansatz auszulegen

17 Ausgangspunkt der Überlegungen ist die **Definition des Art. 2 Buchstabe a der Richtlinie 95/46**: Hiernach bezeichnet der Ausdruck „personenbezogene Daten" alle Informationen über eine bestimmte oder bestimmbare natürliche Person („betroffene Person").

18 Da aus der IP-Adresse selbst nicht erkennbar ist, welche natürliche Person sich dahinter verbirgt, handelt es sich bei einer dynamischen IP-Adresse nicht um eine Information über eine **bestimmte** Person. Für die Beantwortung der ersten Vorlagefrage entscheidend ist daher, ob es sich um eine Information über eine bestimmbare natürliche Person handelt.

19 Als **bestimmbar** wird nach Art. 2 Buchstabe a der Richtlinie 95/46 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. Weitere Anhaltspunkte ergeben sich aus **Erwägungsgrund 26 Satz 2 der Richtlinie 95/46**: Danach sollten „bei der Entscheidung, ob eine Person bestimmbar ist, [...] 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."

20 Der **Bundesgerichtshof** hat im Vorlagebeschluss ausführlich dargelegt, dass in der deutschen Rechtsprechung und Literatur umstritten ist, ob bei der Prüfung der Bestimmbarkeit ein objektiver oder ein relativer Maßstab zugrunde zu legen ist: Nach dem objektiven bzw. absoluten Ansatz kommt es auf die individuellen Verhältnisse der verarbeitenden Stelle nicht an.[2] Da zwar nicht der Homepage-Betreiber, jedoch der Zugangsanbieter über die Daten für die Zuordnung der IP-Adresse zum Anschlussinhaber verfüge, sei die Personenbezogenheit von IP-Adressen generell zu bejahen.[3]

21 Nach dem überwiegend vertretenen relativen Ansatz ist ein Personenbezug zu verneinen, wenn die Bestimmung des Betroffenen für die verantwortliche Stelle mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft verbunden ist, so dass das Risiko einer Identifizierung als praktisch irrelevant erscheint.[4] Für den Fall der IP-

---

[2] Vgl. Bundesgerichtshof, Vorlagebeschluss, Rn. 24 mit weiteren Nachweisen.

[3] Vgl. Bundesgerichtshof, Vorlagebeschluss, Rn. 30.

[4] Vgl. Bundesgerichtshof, Vorlagebeschluss, Rn. 25 mit weiteren Nachweisen.

Adressen bedeutet dies, dass eine Person als bestimmbar angesehen wird, wenn die für die Herstellung des Personenbezugs notwendigen Daten technisch und vor allem auch rechtlich zulässig mit verhältnismäßigem Aufwand erlangt und mit den eigenen Protokolldaten zusammengeführt werden können.[5] Nach dem relativen Ansatz seien, so der Bundesgerichtshof, IP-Adressen alleine zwar für den Zugangsanbieter, nicht aber für den Homepage-Betreiber personenbezogene Daten, da der Homepage-Betreiber den Nutzer nicht ohne unverhältnismäßigen Aufwand identifizieren könne.[6] Die relative Ansicht kann also zur Folge haben, dass dieselben Daten für eine Stelle personenbezogen und für eine andere Stelle nicht personenbezogen sind.[7]

22 Nach Kenntnis der Bundesregierung musste sich der **Gerichtshof** in seiner Rechtsprechung bisher mit dieser Frage noch nicht auseinandersetzen und insbesondere noch nicht damit, unter welchen Voraussetzungen ein Mittel als „vernünftigerweise" im Sinne des Erwägungsgrundes 26 Satz 2 der Richtlinie 95/46 angesehen werden kann. Insbesondere stellte sich diese Frage nicht in der Entscheidung des Gerichtshofs in der Rechtssache *Scarlet Extended*:[8] Dort ging es nämlich nicht um einen Diensteanbieter, sondern um den Internetzugangsanbieter selbst, der sowohl über IP-Adressen als auch über weitere Daten über die Identität seiner Kunden verfügte. Dieser besaß also ohne weiteres selbst sämtliche Mittel für die Bestimmung der betreffenden Person, so dass der Gerichtshof ohne weiteres bejahen konnte, dass es sich bei der Verarbeitung von IP-Adressen durch einen Internetzugangsanbieter um die Verarbeitung von personenbezogenen Daten handelte. Nicht Gegenstand der Entscheidung *Scarlet Extended* war hingegen die Frage, ob IP-Adressen auch für jemanden, der selbst keine Kenntnis über die Identität der Kunden hat (wie z.B. den Diensteanbieter von Internetportalen, d.h. als Serverbetreiber oder Inhalteanbieter) personenbezogene Daten sind. Die Frage war für diese Entscheidung nicht relevant und es wurden hierzu vom Gerichtshof auch keine Aussagen getroffen.

23 Nach Auffassung der **Bundesregierung** ist bei der Prüfung der „Bestimmbarkeit einer Person" ein relativer Maßstab anzulegen. Dies entspricht auch der weit überwiegenden Auffassung in der deutschen Rechtsprechung und Literatur.[9]

---

[5] Vgl. in diesem Sinne LG Berlin, ZD 2013, 618.

[6] Vgl. Bundesgerichtshof, Vorlagebeschluss, Rn. 31.

[7] Vgl. Bundesgerichtshof, Vorlagebeschluss, Rn. 26.

[8] Urteil vom 24. November 2011, *Scarlet Extended*, C-70/10, EU:C:2011:771, Rn. 51.

[9] Vgl. bspw. AG München, ZUM-RD 2009, 413, 414; LG Wuppertal, MMR 2011, 65; LG Berlin, ZD 2013, 618; Simitis/Dammann, in: Simitis, BDSG, 8. Aufl. 2014, § 3 Rn. 23-25; Plath/Schreiber, in: Plath, BDSG, 2013, § 3 Rn. 14 f.; Gola/Klug/Körffer, in: Gola/Schomerus, BDSG, 12. Aufl. 2015, § 3

24 Aus Sicht der Bundesregierung sprechen die Auslegung nach dem Wortlaut (a) und nach Sinn und Zweck der Richtlinie sowie im Lichte der betroffenen Grundrechte (b) für diesen relativen Maßstab:

a) Auslegung nach dem Wortlaut

25 Ausgangspunkt der Überlegungen ist der Wortlaut des Art. 2 Buchstabe a der Richtlinie 95/46, wonach eine Person dann als bestimmbar angesehen wird, wenn sie direkt oder indirekt identifiziert werden kann. Entscheidende Anhaltspunkte hierfür enthält die Formulierung des Erwägungsgrundes 26 Satz 2 der Richtlinie 95/46: Danach sollten bei der Entscheidung, ob eine Person bestimmbar ist, 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.

26 Aus dieser Formulierung lassen sich für die Frage, ob eine Person bestimmbar ist, insbesondere die **folgenden Rückschlüsse ziehen**:

- Erstens wird mit der Formulierung klargestellt, dass nicht alle Mittel schlechthin Berücksichtigung finden, sondern nur diejenigen Mittel, die die dort genannten Voraussetzungen erfüllen.
- Zweitens kommen nicht nur Mittel des von dem für die Verarbeitung Verantwortlichen, sondern grundsätzlich auch Mittel von Dritten in Betracht.
- Drittens ist Voraussetzung für die Heranziehung von Mitteln, dass diese Mittel vernünftigerweise eingesetzt werden könnten, um die betreffende Person zu bestimmen.

27 Insbesondere durch die Worte „vernünftigerweise ... eingesetzt werden könnten" werden die in Betracht kommenden Mittel begrenzt. Hätte der Gesetzgeber gewollt, dass ein Personenbezug bereits dann angenommen wird, wenn eine Bestimmung durch irgendeinen Dritten objektiv möglich ist, wäre die gewählte Formulierung überflüssig.

28 Die Frage, ob ein Mittel „vernünftigerweise" in Betracht zu ziehen ist, kann schon nach dem Wortsinn **nicht losgelöst von der konkret zugrundeliegenden Konstellation**

Rn. 10a; Eckhardt, CR 2011, 339, 342; Meyerdierks, MMR 2009, 8, 9; Krüger/Maucher, MMR 2011, 433, 439.

beantwortet werden. Wenn sich hierbei nun herausstellt, dass ein Mittel eines Dritten zwar rein theoretisch denkbar wäre, jedoch beispielsweise technische oder rechtliche Hindernisse bestehen oder der Aufwand (bspw. an Zeit, Kosten oder Arbeitskraft) völlig außer Verhältnis zum Nutzen steht, dann wird dieses Mittel vernünftigerweise auch nicht eingesetzt werden. Hierfür spricht auch schon die Bedeutung des Begriffs „vernünftigerweise": „Vernünftigerweise" ist eben etwas vollkommen anderes als „rein theoretisch".

b) Auslegung nach Sinn und Zweck sowie im Lichte der betroffenen Grundrechte

29 Eine Auslegung nach **Sinn und Zweck der Richtlinie 95/46** führt nach Auffassung der Bundesregierung ebenfalls zu einem relativen Verständnis.

30 Nach Art. 1 Abs. 1 der Richtlinie 95/46 gewährleisten die Mitgliedstaaten nach den Bestimmungen dieser Richtlinie den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten. Auch im zweiten und dritten Erwägungsgrund der Richtlinie wird auf die Grundrechte und insbesondere die Privatsphäre natürlicher Personen Bezug genommen. Die Richtlinie dient also dazu, die Gewährleistung dieser Grundrechte durch die Mitgliedstaaten sicherzustellen, und gestaltet das Grundrecht auf Privatsphäre bzw. auf Schutz personenbezogener Daten sekundärrechtlich aus.

31 Das Grundrecht auf Schutz personenbezogener Daten ist in Art. 8 EMRK (Schutz der Privatsphäre) enthalten und inzwischen auch in Art. 7 der Charta der Grundrechte (Schutz der Privatsphäre) und explizit in Art. 8 der Charta der Grundrechte geregelt. Auch in Art. 16 AEUV heißt es, dass jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten hat. Allerdings konkretisieren diese Regelungen den Begriff der personenbezogenen Daten nicht näher. Auch im Rahmen dieser Regelungen stellt sich daher die Frage, unter welchen Voraussetzungen es sich um personenbezogene Daten handelt.

32 Nach Auffassung der Bundesregierung ist der Begriff „personenbezogene Daten" in der Richtlinie 95/46 ebenso zu verstehen ist wie in diesen Grundrechten. Hierfür spricht nicht nur die enge Bezugnahme der Richtlinie auf die zugrundeliegenden Grundrechte, sondern vor allem die Tatsache, dass sowohl der Gerichtshof bei der Auslegung der Art. 7, 8 der Charta der Grundrechte als auch der Europäische Gerichtshof für Menschenrechte bei der Auslegung von Art. 8 EMRK davon ausgehen, dass unter perso-

nenbezogenen Daten jede Information zu verstehen ist, die eine bestimmte oder bestimmbare natürliche Person betrifft.[10]

33 Es ist offenkundig, dass sich die Situation und das **Schutzbedürfnis** der betroffenen natürlichen Personen völlig unterschiedlich darstellen können, je nachdem, in wessen Hand sich bestimmte Daten befinden und worin der Verarbeitungsvorgang besteht. Befinden sich Daten, aus denen selbst heraus eine Zuordnung der betroffenen Person nicht möglich ist, beispielsweise in der Hand dessen, der über den „Schlüssel" verfügt, ist eine Identifizierung der Person ohne Schwierigkeiten möglich und es besteht ein besonderes Schutzbedürfnis. Daher steht in einer solchen Konstellation auch nicht in Frage, dass es sich um personenbezogene Daten handelt.

34 Völlig anders stellt sich die Situation jedoch dar, wenn dieselben Daten lediglich von einer Person aufbewahrt werden, die selbst nicht über den „Schlüssel" verfügt und ihn realistischerweise auch nicht von einem Dritten erhalten wird. In einer solchen Konstellation ist nicht ersichtlich, worin die Gefahr einer Identifizierung der betroffenen Person und damit das Schutzbedürfnis bestehen soll.

35 Bereits diese beiden Beispiele zeigen, dass eine Abgrenzung lediglich danach, ob – objektiv betrachtet – irgendjemand rein theoretisch zur Bestimmung der Person in der Lage wäre, für einen angemessenen Schutz der Betroffenen nicht erforderlich ist. Vielmehr ist hierfür ein **relatives Verständnis**, das die konkrete Konstellation berücksichtigt, **völlig ausreichend**.

36 Insbesondere lässt sich hiergegen nicht einwenden, der relative Ansatz könnte zu Schutzlücken führen, da diejenige Person, die die Daten aufbewahrt, ohne über den „Schlüssel" zu verfügen, diese Daten nun ohne weiteres an den „Schlüsselinhaber" übermitteln könnte. Bei der Übermittlung dieser Daten an den „Schlüsselinhaber" wäre vernünftigerweise damit zu rechnen, dass die Person mit Mitteln des „Schlüsselinhabers" identifiziert wird. Folglich handelt es sich in dieser Konstellation um personenbezogene Daten und der Schutz der Richtlinie würde eingreifen. Dies zeigt, dass auch bei einem relativen Verständnis **keine Schutzlücke besteht**.

37 Außerdem ist zu berücksichtigen, dass auch die **Grundrechte weiterer Beteiligter** berührt sein können: Auch die Tätigkeiten datenverarbeitender Stellen können – je nach Konstellation im konkreten Einzelfall – grundrechtlich geschützt sein, beispielsweise

---

[10] Vgl. Urteil des Gerichtshofs vom 9. November 2010, *Volker und Markus Schecke und Eifert*, verb. Rs. C-92/09 und C-93/09, EU:C:2010:662, Rn. 52 mit weiteren Nachweisen.

durch die Berufsfreiheit bzw. die unternehmerische Freiheit (Art. 15, 16 der Charta der Grundrechte). Außerdem können auch Bezüge zum freien Datenverkehr und den Grundfreiheiten des AEUV, insb. zum freien Waren-, Dienstleistungs- und Kapitalverkehr bestehen. Diese Aspekte sind bei der Auslegung der Richtlinie 95/46 ebenfalls zu berücksichtigen. Auch dies spricht dafür, den Begriff der personenbezogenen Daten im Sinne von Art. 2 Buchstabe a der Richtlinie 95/46 nicht weiter zu verstehen als das Schutzbedürfnis der von der Datenverarbeitung Betroffenen reicht.

2. Im Fall der Speicherung von dynamischen IP-Adressen durch Diensteanbieter liegt keine „Bestimmbarkeit" vor

38 Bei der Entscheidung, ob eine Person bestimmbar ist, sind nach Erwägungsgrund 26 Satz 2, wie bereits dargestellt, alle Mittel zu berücksichtigen, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen. Dabei kommt es, wie bereits dargestellt, insbesondere darauf an, ob die für die Herstellung des Personenbezugs notwendigen Daten technisch und rechtlich und mit verhältnismäßigem Aufwand erlangt werden können.

39 Nach Auffassung der Bundesregierung ist das Merkmal der „Bestimmbarkeit" bei der Speicherung von dynamischen IP-Adressen durch Diensteanbieter in einer Konstellation wie der des Ausgangsverfahrens nicht schon dann erfüllt, wenn ein Dritter (hier: Internetzugangsanbieter) über das zur Identifizierung der betroffenen Person erforderliche Zusatzwissen verfügt.

40 Das Zusatzwissen, das dem Internetzugangsanbieter vorliegt, ist nach Auffassung der Bundesregierung nicht als Mittel im Sinne von Erwägungsgrund 26 Satz 2 der Richtlinie 95/46 zu qualifizieren, das vernünftigerweise eingesetzt werden könnte, um die betreffenden Nutzer zu bestimmen. Der Internetzugangsanbieter ist schon aufgrund rechtlicher Vorgaben daran gehindert, dem Diensteanbieter, der die IP-Adressen speichert, die Daten zur Entschlüsselung des Nutzers zu übermitteln (siehe dazu sogleich).

41 Der Verneinung des Personenbezugs im Falle der Speicherung von IP-Adressen durch einen Diensteanbieter steht insbesondere die Entscheidung des Gerichtshofs in der Rechtssache *Scarlet Extended*[11] nicht entgegen. Wie bereits in Rn. 22 dargestellt, trifft diese Entscheidung keinerlei Aussagen darüber, ob IP-Adressen für einen Diensteanbieter

[11] Urteil vom 24. November 2011, *Scarlet Extended*, C-70/10, EU:C:2011:771, Rn. 51.

bieter, der IP-Adressen speichert, aber selbst keine Kenntnis über die Identität der Nutzer hat, als personenbezogene Daten zu qualifizieren sind oder nicht.

42 Ebenso wie die Bundesregierung kommt der Bundesgerichtshof bei Zugrundelegung eines relativen Ansatzes zu dem Ergebnis, dass der Personenbezug im Streitfall zu verneinen ist, da die Stellen der beklagten Bundesregierung, die die IP-Adressen des Klägers gespeichert haben, den Kläger nicht ohne unverhältnismäßigen Aufwand identifizieren könnten.[12]

43 Diensteanbietern (Serverbetreibern oder Inhalteanbietern) ist es in einer Konstellation wie der vorliegenden grundsätzlich weder technisch noch rechtlich möglich, einen Personenbezug herzustellen.

44 Die Zuordnung einer dynamischen IP-Adresse lässt sich nicht einer allgemein zugänglichen Datei entnehmen.[13] Aus den von den Internetportalen der Beklagten in Protokolldateien gespeicherten Einzeldaten, bestehend aus Name der abgerufenen Datei und/oder Seite, in Suchfelder eingegebene Begriffe, Zeitpunkt des Abrufs, übertragene Datenmenge, Meldung, ob Abruf erfolgreich war, und die dynamische IP-Adresse des zugreifenden Rechners, lässt sich kein unmittelbarer Rückschluss auf die Identität des Nutzers ziehen. Entscheidend ist, dass IP-Adressen **nur in Verbindung mit Zusatzinformationen** ein Teil von personenbezogenen Daten werden können, für sich alleine aber keine solche Daten sind.

45 Der Bundesgerichtshof führt in Rn. 32 seines Vorlagebeschlusses nach Auffassung der Bundesregierung zutreffend aus, dass der Zugangsanbieter des Klägers **der Bundesrepublik Deutschland als Beklagten, die die IP-Adressen speichern, keine Auskunft über dessen Identität erteilen durfte**, weil es dafür keine gesetzliche Grundlage gibt. Nach § 95 Abs. 1 S. 3 des Telekommunikationsgesetzes (TKG) darf eine Übermittlung der Bestandsdaten an Dritte, soweit nicht ein Gesetz sie zulässt, nur mit Einwilligung des Teilnehmers erfolgen.

46 Weiterhin weist der Bundesgerichtshof in Rn. 32 nach Auffassung der Bundesregierung zutreffend darauf hin, dass alleine die rechtlich explizit eingeräumten Befugnisse der zuständigen Stellen nach § 113 TKG (wie etwa der Staatsanwaltschaft in einem Ermittlungsverfahren) es **nicht** rechtfertigen, die aufgrund dieser Befugnisse beschaffbaren Informationen auch für **andere staatliche Stellen** (wie etwa den Stellen der

---

[12] Bundesgerichtshof, Vorlagebeschluss, Rn. 31.

[13] Bundesgerichtshof, Vorlagebeschluss, Rn. 31 a.E..

Bundesrepublik Deutschland, die als Serverbetreiber oder Anbieter von Telemedien die IP-Adressen speichern), an die diese Informationen nicht weitergegeben werden dürfen, als zugänglich anzusehen. Die Bundesregierung ist ebenfalls der Auffassung, dass hier eine „Zurechnung" des Wissens einer staatlichen Stelle auf alle staatlichen Stellen der Bundesrepublik Deutschland und der Länder der Bundesrepublik Deutschland oder gar auf alle öffentlichen Stellen nicht angemessen und auch nicht mit den geltenden Regelungen vereinbar wäre: In § 113 TKG wird explizit angeordnet, dass die entsprechenden Daten auch nicht an andere öffentliche Stellen als die dort genannten übermittelt werden dürfen. Darüber hinaus nennt die Definition des „für die Verarbeitung Verantwortlichen" in Art. 2 Buchstabe d der Richtlinie 95/46 neben natürlichen und juristischen Personen, Einrichtungen und sonstigen Stellen, die allein über die Zwecke und Mittel der Datenverarbeitung entscheiden, ausdrücklich auch Behörden. Hiermit hat der Gesetzgeber der Richtlinie zum Ausdruck gebracht, dass der Staat nicht als eine einzige Stelle, die für die Verarbeitung verantwortlich ist, anzusehen ist, deren Wissen zusammengerechnet werden muss. Vielmehr betrachtet er die verschiedenen staatlichen organisatorischen Einheiten getrennt.

47 Außerdem führt der Bundesgerichtshof zu Recht aus, dass **illegale Handlungen** nicht als Mittel der Informationsbeschaffung angesehen werden können.[14] Nach Auffassung der Bundesregierung ergibt sich dies bereits aus der Formulierung von Erwägungsgrund 26 Satz 2 der Richtlinie 95/46: Vernünftigerweise ist eben nicht zu erwarten, dass Zugangsprovider und/oder Diensteanbieter illegale Mittel verwenden, also Daten illegal weitergeben bzw. sich diese illegal beschaffen. Zwar lässt sich nie völlig ausschließen, dass nicht doch irgendwo ein Fall illegalen Handels auftreten könnte; dies gilt aber nicht nur für den Bereich der Beschaffung von Daten, die hinter IP-Adressen stehen, sondern ganz generell für jeden Lebensbereich, und kann insbesondere nicht dazu führen, dass illegale Mittel nun als „vernünftigerweise" einzusetzendes Mittel zu qualifizieren wären.

48 Im Übrigen hat der Gerichtshof einen ähnlichen Gedanken bereits in seinem Urteil *Markus Stoß u.a.*[15] zum Glücksspielrecht herangezogen: In den verbundenen Rechtssachen C-316/07 u.a. hat der Gerichtshof eine Argumentation abgelehnt, die die staatlichen Glücksspielmonopole als unionsrechtswidrig qualifizieren wollte, weil sie angesichts über das Internet vorgenommener unzulässiger Transaktionen nicht effizient

---

[14] Bundesgerichtshof, Vorlagebeschluss, Rn. 32.

[15] Urteil vom 8. September 2010, *Markus Stoß u.a.*, verb. Rs. C-316/07, C-358/07 bis C-360/07, C-409/07 und C-410/07, EU:C:2010:504, Rn. 84 ff.

seien. Auch Generalanwalt Mengozzi hatte in seinen Schlussanträgen ausgeführt, eine Beschränkung in nationalen Vorschriften sei als solche mit dem Vertrag vereinbar oder nicht, und die Möglichkeit, diesen nationalen Regeln zuwiderzuhandeln, insoweit unerheblich.[16]

49 Schließlich weist der Bundesgerichtshof in seinem Vorlagebeschluss darauf hin, dass es **erst recht bei staatlichen Stellen** gelten müsse, dass illegale Handlungen nicht als Mittel der Informationsbeschaffung angesehen werden können. In diesem Zusammenhang sei daher besonders auf die im deutschen Grundgesetz verankerte Gesetzesbindung der Verwaltung und das Rechtsstaatsprinzip hingewiesen, das im Übrigen auch Teil des Unionsrechts ist (vgl. Art. 2 EUV).

50 Im Ergebnis ist also in einer Konstellation wie der des Ausgangsverfahrens die „Bestimmbarkeit" und damit auch der Personenbezug zu verneinen. Daher ist die erste Vorlagefrage aus Sicht der Bundesregierung **zu verneinen**.

II. Zur zweiten Vorlagefrage

51 Die Beantwortung der zweiten Vorlagefrage erübrigt sich, da sie nur für den Fall der Bejahung der ersten Vorlagefrage gestellt wurde.

E. ERGEBNIS

52 Vor diesem Hintergrund schlägt die Bundesregierung vor, die Vorlagefrage wie folgt zu beantworten:

---

[16] Vgl. Schlussanträge des Generalanwalts Mengozzi vom 4. März 2010, *Markus Stoß u.a.*, verb. Rs. C-316/07, C-358/07 bis C-360/07, C-409/07 und C-410/07, EU:C:2010:109, Rn. 79.

Art. 2 Buchstabe 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 (ABl. EG 1995, L 281/31) - Datenschutz-Richtlinie - ist dahin auszulegen, dass in einer Konstellation wie der des Ausgangsverfahrens eine dynamische Internetprotokoll-Adresse (IP-Adresse), die ein Diensteanbieter im Zusammenhang mit einem Zugriff auf seine Internetseite speichert, nicht bereits dann ein personenbezogenes Datum darstellt, wenn nur ein Internetzugangsanbieter über das zur Identifizierung der betroffenen Person erforderliche Zusatzwissen verfügt.